

ZoneAlarm™ PRO 3.0

User's Manual

© 2002 Zone Labs, Inc. All Rights Reserved. TrueVector, ZoneAlarm, Zone Labs, the Zone Labs logo and Zone Labs Integrity are either registered trademarks or trademarks of Zone Labs, Inc. Cooperative Enforcement and Policy Lifecycle Management are service marks of Zone Labs, Inc. All other trademarks are the property of their respective owners.

Zone Labs Inc., 1060 Howard Street, San Francisco, CA 94103. USA.

1 **Introduction** **9**

Welcome to ZoneAlarm Pro 3.0	9
How this guide is organized	9

2 **How ZoneAlarm Pro protects you** **11**

Firewall protection	11
What's a firewall?	11
What are ports?.....	11
What is a protocol?	12
How does it work?	12
What is a Zone?	12
How does the firewall use Zones and security levels?	13
Program Control	14
Why do I need program control?	14
Program authentication	14
Program access control.....	15
Privacy protection	15
Cookie control	16
Ad blocking	16
Mobile Code control.....	17
Privacy Advisor.....	18
Privacy per program.....	18
Alerts & Logs	18
Controlling the display of alerts	18
Logging security events.....	19
E-mail protection	19

3 **Installing ZoneAlarm Pro** **21**

System Requirements	21
Easy installation	21
Installation screen 1: Choose an install location	22
Installation Screen 2: Personal Information	22

Installation Screen 3: Upgrade or clean install?	23
Installation Screen 4: License Agreement	24
Installation screen 5: User survey	25
Installation screen 6: Try or buy dialog	26
Configuration Wizard.....	26
Configuration Wizard 1: Welcome	27
Configuration Wizard 2: Review Privacy settings.....	28
Configuration Wizard 3: Review Firewall Alert Settings (Optional)	29
Configuration Wizard 4: Create a password	30
Configuration Wizard 5: Configure for ICS	31
Configuration Wizard 6: Preconfigure Browser	32
Configuration Wizard 7: Secure Programs	33
Configuration Wizard 8: Congratulations!.....	34

4 Using ZoneAlarm Pro **35**

Setting up.....	35
Should I change the default security settings?	35
Should I engage the Internet Lock?.....	35
How do I know ZoneAlarm Pro is working?	35
What do alerts mean?	35
How do I set up for my network?.....	35
How do I customize my security?.....	36
Choosing Security Settings.....	36
Security and convenience	36
ZoneAlarm Pro default settings	36
Responding to Alerts.....	38
New Network alerts.....	39
New Program alerts	40
Firewall alerts	41
Other alerts.....	43
Repeat Program alert	43
Server Program alert	44
Changed Program alert	45
Program Component alert	46
Component Loading alert	48
MailSafe alert	49

Internet Lock alerts	51
Blocked Program alerts	52
Investigating changed programs and components.....	53
Investigating changed programs	53
Investigating changed components	53
Using the Internet Lock and Stop button.....	54
What's the difference between Stop and Lock?.....	54
Turning the lock on and off	54
How do I know the Lock is on?	55
Using the Automatic Internet Lock.....	55
Using your programs with ZoneAlarm Pro.....	56
Anti-virus software	56
Browsers	56
Chat/Instant Messaging.....	57
E-mail programs (e.g., MS Outlook)	57
File Sharing	58
FTP	58
Games	58
Internet call waiting/ Internet answering machines	60
Remote control and display	60
Streaming audio/video	61
Voice over IP (VoIP)	62
Networking with ZoneAlarm Pro	62
Making your computer visible on your local network	62
Sharing files and printers across a local network	62
VPN (Virtual Private Network).....	63
ICS (Internet Connection Sharing)	63
Proxy server.....	64
ISP heartbeat	64
Customizing your security.....	65
Firewall protection.....	66
Program control	66
Alerts and logs.....	66
Privacy protection	67
E-mail protection.....	67
Reading the ZoneAlarm Pro log.....	67

Viewing the Log	67
Log fields	68
Event types	69
ICMP message types	69
TCP flags	70
Sample log entries	70
5 Interface Guide.....	73
The ZoneAlarm Pro dashboard	73
Inbound/Outbound traffic indicator	73
Stop button (Emergency Panic Lock)	73
Networks.....	73
Internet Lock	74
Active programs.....	74
All systems active	74
Overview Panel.....	75
Status tab.....	75
Product Info tab	77
Preferences tab	79
Firewall panel.....	81
Main tab	81
Zones tab	82
Internet Zone tab	84
Trusted Zone tab	86
Security tab	88
Program Control panel.....	90
Main tab	90
Programs tab.....	92
Components tab	95
Auto-lock tab	98
Access Permissions tab	99
Alerts & Functionality tab.....	100
Ports tab	102
Security tab	104
Alerts & Logs panel.....	105
Log Viewer tab	106

Program Logs tab	109
Alert Events tab	110
System Tray Alert tab	111
Log Control tab	113
Privacy Panel.....	115
Main tab	115
Site List tab	117
Cookies tab	119
Ad Blocking tab	121
Mobile Code tab	122
E-mail Protection panel.....	123
Main tab	123
Attachments tab.....	123

6 Glossary **125**

A	125
B	126
C	127
D	127
E	128
F.....	128
G.....	128
H.....	129
I.....	129
J.....	130
K	130
L.....	130
M.....	131
N	132
O.....	132
P	132
Q.....	134
R	135
S	135
T.....	136
U	137

V	137
W	137
XYZ	137

1 Introduction

Welcome to ZoneAlarm Pro 3.0

Thank you for choosing ZoneAlarm Pro!

ZoneAlarm Pro is the award-winning personal firewall that blocks known and unknown Internet threats such as hackers, data thieves, spyware, and e-mail-borne worms. ZoneAlarm Pro 3.0 provides new privacy protections, too, including ad blocking and cookie control. With ZoneAlarm Pro, whenever you're connected, you're protected.

With the new and enhanced features in ZoneAlarm Pro 3.0, you get:

- Comprehensive security with the most-popular personal firewall—*plus* advanced privacy features.
- A barricade against known *plus* unknown Internet threats—including hackers, data thieves, spyware, and email borne worms—that goes beyond other Internet security solutions.
- Program Control to prevent unauthorized inbound *plus* outbound connections—stopping rogue applications from transferring your valuable data to a hacker.
- Robust security that protects you right out of the box—*plus* the ability to customize security controls to match your specific requirements and preferences.
- Comprehensive protection for standalone or networked computers—*plus* full protection for mobile computers.
- Advanced email protection that prevents your computer from being infected by or inadvertently spreading malicious code—*plus* enhanced hacker tracking allows you to pinpoint the origins of would-be intrusions.

How this guide is organized

This guide contains information that will help you use ZoneAlarm Pro effectively. Here's how it's organized:

- **Chapter 2 (How ZoneAlarm Pro protects you)** provides an overview of ZoneAlarm Pro's major security features. Use this chapter to learn the basics of Internet security and how ZoneAlarm Pro protects you from threats.
- **Chapter 3 (Installing ZoneAlarm Pro)** shows you how to install ZoneAlarm Pro and how to use the Configuration Wizard to choose basic security settings.

- **Chapter 4 (Using ZoneAlarm Pro)** covers major tasks you may need to perform while using ZoneAlarm Pro. Use this chapter to learn how to respond to alerts, how to set up ZoneAlarm Pro for your network, and so forth.
- **Chapter 5 (Interface Guide)** is a panel-by-panel reference guide to the ZoneAlarm Pro control center. Use this chapter to find out what each control in the user interface does.

2

How ZoneAlarm Pro protects you

ZoneAlarm pro offers four main lines of defense against Internet threats:

- **Firewall protection** guards the “doors” (ports) through which hackers can break in to your computer.
- **Program control** keeps Trojan horses and other hacker malware from setting up shop on your computer.
- **Privacy protection** protects your personal information from the abuse of Internet cookies and advertisements, and protects you from possibly dangerous mobile code (scripts and embedded objects) buried in Web pages.
- **E-mail Protection** shields you from worms and viruses (both known and unknown) that can arrive in e-mail attachments.

Firewall protection

What's a firewall?

In buildings, a firewall is a barrier that prevents a fire from spreading. In computers, the concept is similar. There are a variety of "fires" there out on the Internet—hacker activity, viruses, worms, and so forth. A firewall is a system that stops the fire from spreading to your computer.

A firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. The firewall only lets traffic through the ports that you have specified can be used. This has two security benefits:

- No one can sneak into your computer through an unguarded port.
- Programs on your computer can't use unguarded ports to contact the outside world without your permission.

What are ports?

Ports are logical channels through which traffic enters or leaves your computer. Your computer has thousands of ports, each identified by a number.

Whenever another computer sends a message to your computer, it addresses that message to a specific port. For example, a server delivering a Web page to your browser, using the Hypertext Transfer Protocol (HTTP), traditionally sends to port 80.

What is a protocol?

A protocol is a bit like a language—it is an agreed-on way of transmitting information. The Internet uses many protocols, and each of them is normally associated with a particular port or ports. For example, the NetBIOS protocol, which is used by Windows systems to enable resource sharing on a local network, traditionally uses ports 135, 137-39, and 445.

How does it work?

All Internet traffic—Web pages, e-mail, audio files, and so on—are transmitted in bite-sized chunks called "packets." Each packet is addressed to a particular computer, and to a particular port on that computer.

ZoneAlarm Pro examines every packet that arrives at your computer and asks four questions:

1. What Zone did the message come from? Trusted, Internet, or Blocked?
2. What port is it addressed to?
3. Do the rules for that Zone allow traffic through that port?
4. Are there any other rules the packet violates? (Fragmented, source-routed, etc.?)

Block incoming NetBIOS (ports 135,137-9,445) If yes, the packet is allowed in.

Block incoming NetBIOS (ports 135,137-9,445) If no, the packet is blocked.

Note This describes the treatment of unsolicited traffic—that is, packets that arrive from the Internet or a local network unexpectedly. Port scans are a good example of unsolicited traffic that ZoneAlarm Pro protects you from. When a permitted program on your computer has established a communications session with another computer, Program Control rules decide what ports can be used.

What is a Zone?

Zones are how ZoneAlarm Pro keeps track of the **good**, the **bad**, and the **unknown** out on the Internet.

Zones are virtual spaces

Zones are virtual spaces—ways of classifying the computers and networks that your computer communicates with.

- **The Internet Zone** is the "unknown." All the computers and networks in the world belong to this Zone—until you move them to one of the other Zones.
- **The Trusted Zone** is the "good." It contains all the computers and networks you trust and want to share resources with—for example, the other machines on your local or home network.
- **Blocked Zone** is the "bad." It contains computers and networks you distrust.

When another computer wants to communicate with your computer...

ZoneAlarm Pro looks at the Zone it is in—that is, whether it is **good**, **bad**, or **unknown**—to help decide what to do.

Tip To put a computer or network in the Trusted Zone, use the Zones tab. See page 82.

Zones organize firewall security

By default, ZoneAlarm Pro applies **High** security to the Internet Zone and **Medium** security to the Trusted Zone. You are safe from hackers out on the Internet, but you can share resources with the computers and networks you trust. **No** security level is necessary for the Blocked Zone, because NO traffic to or from that Zone is allowed. Using controls in the Firewall panel, you can adjust the security level for each Zone.

Tip Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. See *Internet Zone tab* and *Trusted Zone tab*, pages 84 and 86.

Zones organize program control

Whenever a program wants access permission or server permission, ZoneAlarm Pro checks in the programs list. Each program has the following permission settings:

- **Access** permission for the **Trusted Zone/Internet Zone**
- **Server** permission for the **Trusted Zone/Internet Zone**

As you use your computer, ZoneAlarm Pro will display a New Program alert whenever a new program wants access or server permission.

To change access and server permissions for a program, use the Programs tab. See page 92.

For definitions of access permission and server permission, see the Glossary on page 125.

How does the firewall use Zones and security levels?

The answer to question number three above ("Do the rules for that Zone allow traffic through that port?") depends on the security level that is applied to each Zone.

To choose a security level for a Zone, use the slider controls in the Main tab of the Firewall panel.

To define the meaning of each security level (that is, the ports that are blocked or allowed at that level) , use the Internet Zone tab and Trusted Zone tab in the Custom Securities dialog box .

Program Control

Program control protects you from Trojan horses and other hacker malware by making sure only programs with your permission can access the Internet.

Why do I need program control?

Everything you do on the Internet—from browsing Web pages to downloading MP3 files— is managed by specific applications (programs) on your computer.

Hackers exploit this fact by planting "malware"—literally, evil programs—on your computer. Sometimes they send out malware as e-mail attachments with innocent names like "screensaver.exe." If you open the attachment, you install the malware on your computer without even knowing it. Other times, they convince you to download the malware from a server by making it masquerade as an update to a legitimate program.

Once on your machine, malware can wreak havoc in a variety of ways. It can raid your address book and mail itself to everyone in it, or it can listen for connection requests from the Internet. The hacker who distributed the malware can then contact it and give it instructions---effectively taking control of your computer.

ZoneAlarm Pro protects you from malware attacks

ZoneAlarm Pro's program control features use two methods to protect you from malware attacks: program authentication and program access control.

Program authentication

Whenever a program on your computer wants to access the Internet, ZoneAlarm Pro authenticates it via its MD5 signature.

What is an MD5 signature?

A digital "fingerprint" used to verify the integrity of a file. If a file has been changed in any way (for example, if a program has been compromised by a hacker), its MD5 signature will change as well.

If the program has been altered since the last time it accessed the Internet, ZoneAlarm Pro displays a Changed Program alert. You decide whether the program should be allowed access or not.

For added security, ZoneAlarm Pro also authenticates the components (for example, DLL files) associated with the program's main executable file. If a component has been

altered, you'll see a Program Component alert--similar in appearance to a changed program alert.

Program access control

When you're using ZoneAlarm Pro, no program on your computer can access the Internet or your local network, or act as a server, unless you give it permission to do so.

When a program requests access for the first time....

A New Program alert asks you if you want to grant the program access permission. If you're not sure whether to click **Yes** or **No**, you can click the **More Info** to have Zone Labs' Alert Advisor help you decide what to do.

A Program Component alert (similar to a new program alert) lets you know if the program is using a component that is new or has changed.

If the same program requests access again....

A Repeat Program alert asks you if you want to grant (or deny) access permission to a program that has requested it before.

Tip To avoid seeing repeat program alerts, select the **Remember this answer** check box near the bottom of the alert before clicking **Yes** or **No**. After that, ZoneAlarm Pro will silently block or allow the program.

When a program asks for server permission...

A Server Program alert asks you if you want grant server permission to a program.

Caution Because Trojan horses and other types of malware often need server rights in order to do mischief, you should be careful to give server permission only to programs that you know and trust, and that need server permission to operate properly.

See also *New Program alert*, page 40, *Repeat Program alert*, page 43, *Program Component alert*, page 46 and *Server Program alert*, page 44.

Privacy protection

ZoneAlarm Pro's privacy protection features, new in version 3.0, shield you from intrusive and potentially dangerous features of Web sites.

Note Privacy protection is enabled for your browser only if you selected it during setup. If you did not enable privacy during setup, you can enable it by going to the Main tab of the Privacy panel and raising the Cookie Control and Ad Blocking sliders to the level you desire.

Cookie control

Cookie control keeps advertisers from spying on your Internet habits. High security settings keep sensitive information (passwords, for example) from being stored in cookies, where they can be stolen if a hacker breaks into your computer.

What is a cookie?

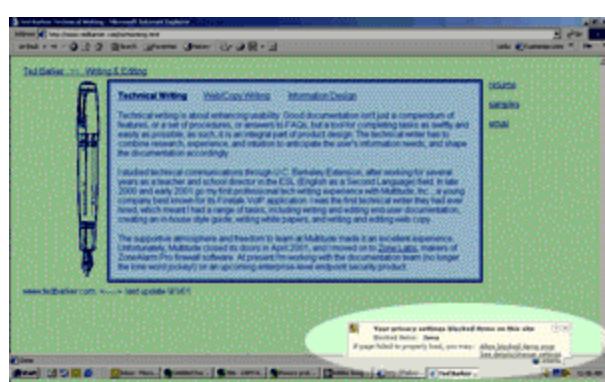
A "cookie" is a small text file that a Web site places on your computer.

A cookie that stays on your computer a long time (called a persistent cookie) lets the Web site remember who you are, so that the next time you visit, it can customize what you see. For example, this is how Amazon.com shows you books you're likely to want each time you visit.

A cookie placed by someone other than the Web site host (called a third-party cookie) can be used to record information about your Internet habits—for example, which advertisements you click on. These cookies are often placed by advertisers.

The default Medium cookie control setting allows session cookies and persistent cookies, but blocks third-party cookies. This protects you from information leaks while preserving the convenient functions of cookies.

When a Web site tries to place a third-party cookie on your computer...



ZoneAlarm Pro blocks the cookie and displays the Privacy Advisor (highlighted at right) at the bottom of your screen. Privacy Advisor tells you that ZoneAlarm Pro has blocked a Web page element.

For more information about the Privacy Advisor, see below.

Tip You can set cookie control to block session and persistent cookies as well. See *Cookies tab*, page 119.

Ad blocking

Ad blocking keeps unwanted advertisements from disrupting your Internet work.

With ZoneAlarm Pro, you can block all types of ads or only specific types:

- Skyscraper and banner ads extend across the top or up the side of the Web page itself.

- Pop/up and pop-under ads appear in a new browser window that "pops up" in front of or under the screen you're looking at.
- Animated Ads use moving images, color changes, and so forth.

When you visit a Web page with ads...

ZoneAlarm Pro blocks pop-up and pop-under ads. It's as if they didn't exist.

ZoneAlarm Pro also blocks banner and skyscraper ads if they take more than a few seconds to load. This is called performance ad blocking, and keeps advertisers from slowing down your Web experience.

Tip You can customize ad blocking to stop block all banner and skyscraper ads, or to stop only specific types of ads. See *Ad Blocking tab*, page 121.

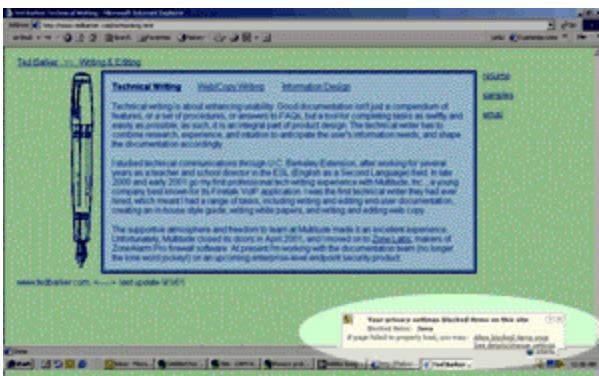
Mobile Code control

Mobile code control keeps hackers from using active Web page content such as Java applets, ActiveX controls and plug-ins to compromise your security or damage your computer.

What is mobile code?

Mobile code is active or executable Web page content. Some examples include Java applets, ActiveX controls, and Javascript. Properly used, mobile code makes Web pages more interactive and dynamic. But malicious mobile code, can copy files, wipe out a hard disk, steal passwords, or command servers.

When you open a Web page that contains mobile code....



ZoneAlarm Pro blocks the code and displays the Privacy Advisor (highlighted at left) at the bottom of your screen. The Advisor tells you that ZoneAlarm Pro has blocked a page element, and gives you access to controls to unblock it for the current Web site if you want to.

For more information about the Privacy Advisor, see below.

Note Mobile code control is turned OFF by default. To turn it on, go to the Overview tab of the Privacy panel.

Tip You can choose to block some types of mobile code and allow others. See *Mobile Code tab*, page 122.

Privacy Advisor



The Privacy Advisor appears whenever ZoneAlarm Pro blocks cookies or mobile code from the Web site you are visiting.

If want to allow the page elements that ZoneAlarm Pro has blocked, click the Advisor pop-up. The ZoneAlarm Pro Control Center opens to the Privacy panel, where you can change general privacy settings, or settings for site you are visiting.

If you don't click the Privacy Advisor pop-up, it disappears automatically in a few seconds. You can also close it by clicking the X in the upper-right corner.

Privacy per program

By default, privacy protection is applied only to standard browser programs such as Internet Explorer. If you wish, you can also enable privacy protection for any other program on your computer by using the Privacy column in the Programs tab. See *Programs tab*, page 92.

Alerts & Logs

ZoneAlarm Pro's alert and logging features keep you aware of what's happening on your computer without being overly intrusive.

Controlling the display of alerts

You may be the type of person who wants to know everything that happens on your computer--or you may not want to be bothered, as long as you know your computer is secure.

ZoneAlarm Pro accommodates you, no matter which kind of person you are. You can be notified by an alert pop-up (shown in reduced size at left) each time ZoneAlarm Pro acts to protect you; or you can opt for quieter protection.

Alert display settings

The default alert display setting (Medium) minimizes interruptions by only showing you alerts that are **high-rated**--that is, that are likely to have resulted from hacker activity.

The **high** alert display setting will show you all alerts—even those probably caused by normal network traffic. If you don't want to be bothered by firewall alerts at all, just select Off.

Tip If you want to change privacy settings for the Web site you are viewing, click the Privacy Advisor. ZoneAlarm Pro will open to the Site List tab, with the site you are viewing selected. Use the controls in the Site List tab to change privacy settings for the site.

Logging security events

You can control logging just as completely as you control alert display, choosing to record all alerts, only high-rated alerts, or alerts caused by specific traffic types.

ZoneAlarm Pro 3.0 gives you easy access to alert log records via the Alert Log tab, so you can quickly retrieve the details on any individual alert.

ZoneAlarm Pro also provides easy tools for formatting and archiving text logs.

E-mail protection

ZoneAlarm Pro's MailSafe™ feature protects you from new viruses, worms, and other malware distributed in e-mail attachments. It also protects you from any old, known threats.

Attaching files to e-mail messages is a convenient way of exchanging information.

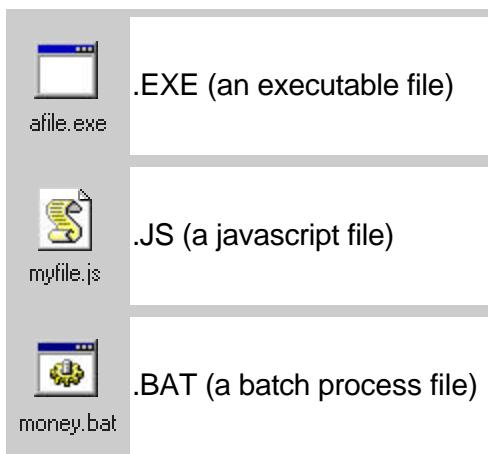
However, it also provides hackers with an easy way of spreading viruses, worms, Trojan horse programs, and other malware. For example, the infamous "Love Bug" worm was distributed as a Visual Basic Script (.VBS) file.

LOVE-LETTER
-FOR-YOU.TXT
VBS

Fortunately, only certain types of attachments can contain potentially dangerous code. These attachments types can be identified by their filename extensions.

About filename extensions

Filename extensions are the characters that appear after the "dot" in a file name. They identify the file type so that the appropriate program or system component can open it. Here are some examples:



Tip It's a good idea never to open an e-mail attachment unless you know the person it came from, and have confirmed (by phone or separate e-mail message) that that person actually sent it to you. Remember hackers can alter an e-mail message to look like it came from a friend!

ZoneAlarm Pro's MailSafe protects you by 'quarantining' e-mail attachments that may contain malicious code.

When an e-mail with an attachment arrives...



MailSafe examines the attachment's filename extension. If that extension (in the example at left, .BAT) is in MailSafe's quarantine list, ZoneAlarm Pro changes the filename extension to ".zl*" (where * is a number or letter.) Changing the filename extension 'quarantines' the attachment by keeping it from running automatically.

When you open the e-mail containing the attachment...



ZoneAlarm Pro displays a MailSafe alert to let you know it has quarantined the attachment. Click **OK** to close the alert box.

When you try to open the attachment...



ZoneAlarm Pro warns you of the potential risk in opening the attachment. If you're sure the file is harmless and you want to open it, click the **Run** button. You can also save the file for later.

Tip Users who know how to read code can click **Inspect with Notepad** to examine the code of attachment itself.

3 Installing ZoneAlarm Pro

System Requirements

The minimum system requirements for ZoneAlarm Pro 3.0 are:

Processor: IBM PC or 100% compatible Pentium® or higher

Operating System: Microsoft Windows 98/ME/NT/2000/XP

Memory: 16 megabytes RAM

Disk space: 10 megabytes

Easy installation

ZoneAlarm Pro is easy to set up and install.

Follow these four simple steps:

1. Download the installer from the Zone Labs Web site (www.zonelabs.com).
2. Close all programs.
3. Launch the installer by double clicking the installer icon (shown at left).
4. Follow the instructions in the installation screens, described below.

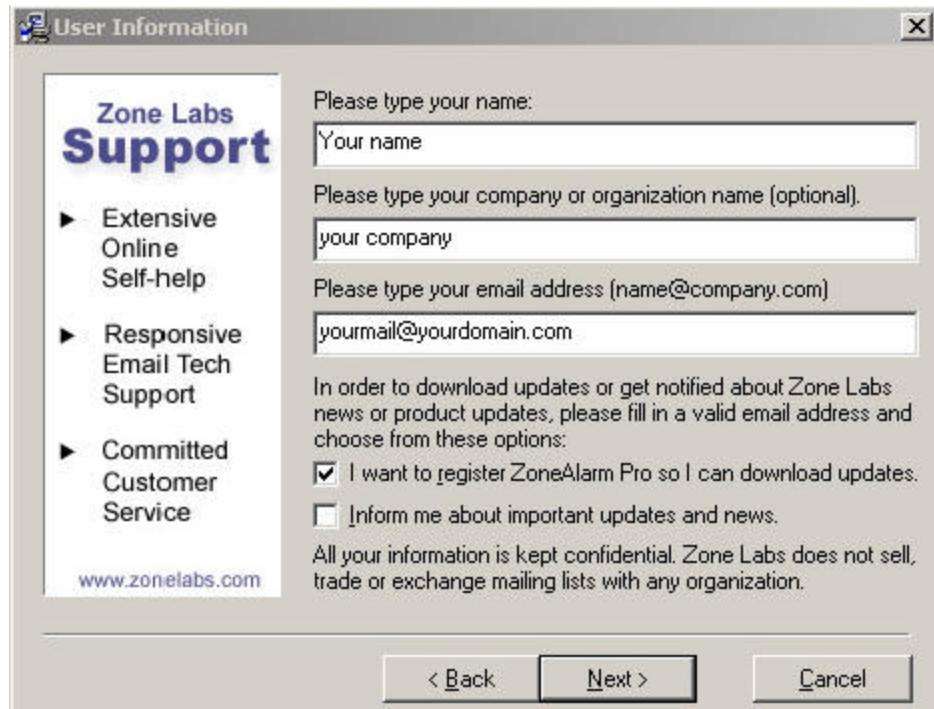


Installation screen 1: Choose an install location



Click **Browse** if you want to change the location in which ZoneAlarm Pro will be stored. Otherwise, click **Next** to go to the next screen.

Installation Screen 2: Personal Information

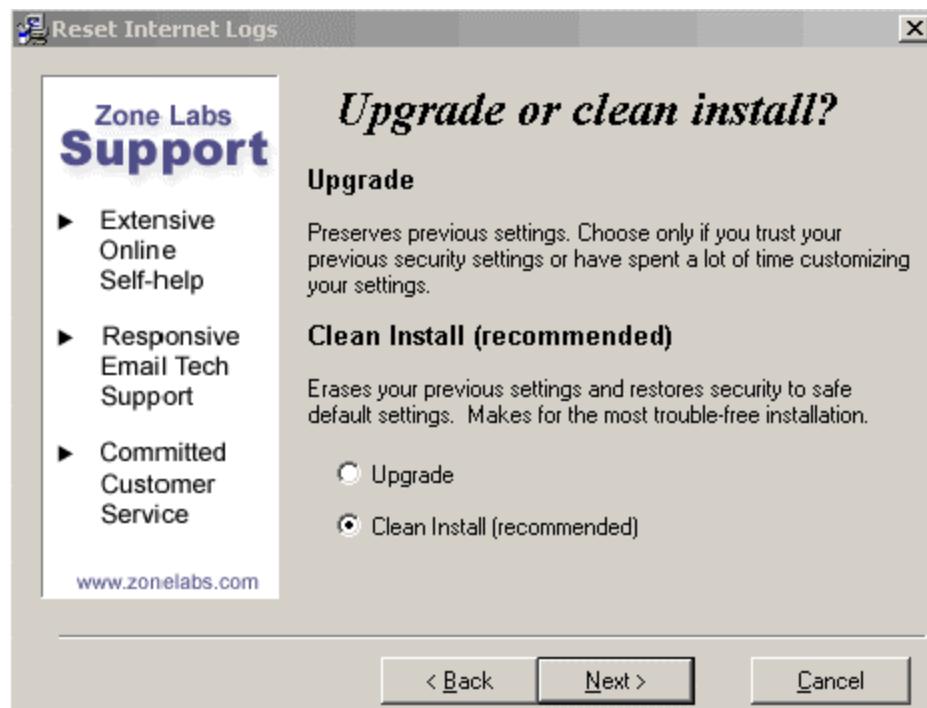


Use this screen to personalize your copy of ZoneAlarm Pro. Type your name, company, and e-mail address in the boxes provided.

- To register the product so that you can receive updates, select the **I want to register...** checkbox.
- To have Zone Labs notify of important security news, select the **Inform me...**checkbox.

Click **Next** when you are finished.

Installation Screen 3: Upgrade or clean install?



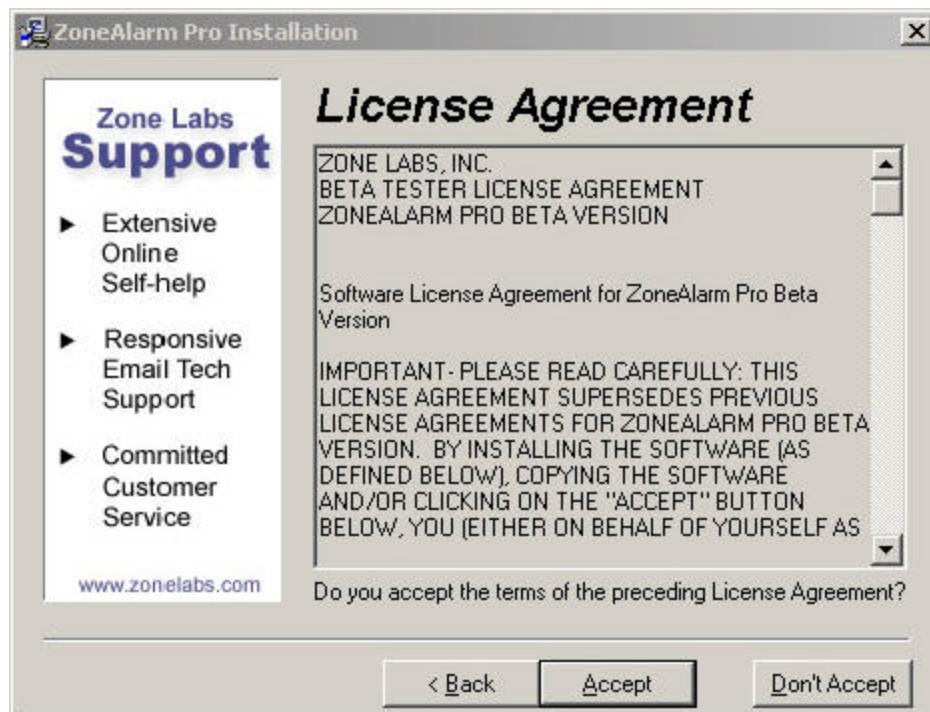
If you had previous version of ZoneAlarm Pro (or a trial version of 3.0), your security settings may still be on your disk even if you have uninstalled the old version.

Tip Unless you have a lot of custom configuration that would take a lot of time to reproduce, choose Clean install. This ensures the smoothest possible installation.

- To keep your old settings, select **Upgrade**
- To start from scratch, select **Clean Install (recommended)**

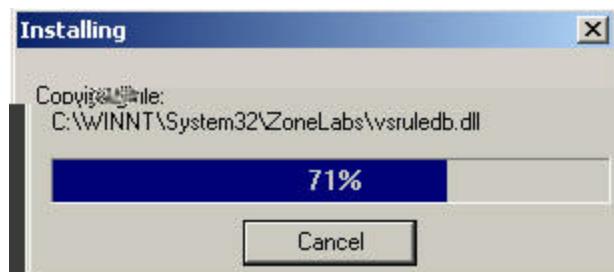
Click **Next** when you are finished.

Installation Screen 4: License Agreement



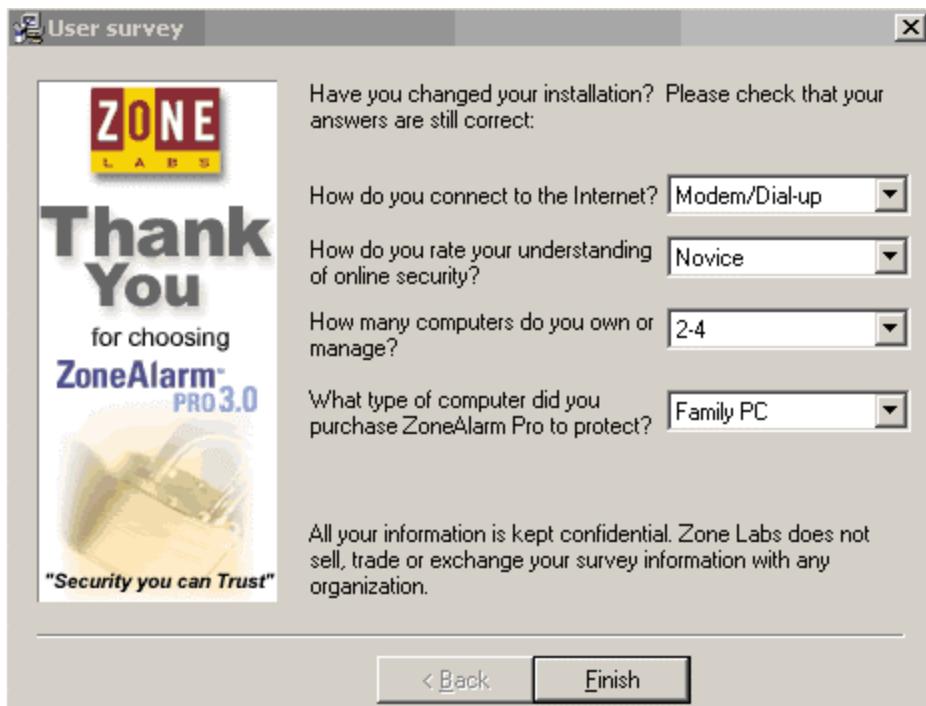
Use the scroll bar to read the full text of your ZoneAlarm Pro license agreement. Click **Accept** to accept the terms of the agreement.

The installer now installs ZoneAlarm Pro. You see the following screen.



When installation is finished, you see the following screen.

Installation screen 5: User survey

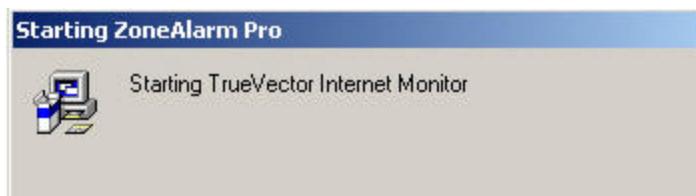


The user survey is optional. It helps Zone Labs better understand the needs of our customers. Please take a few moments to answer the four questions.



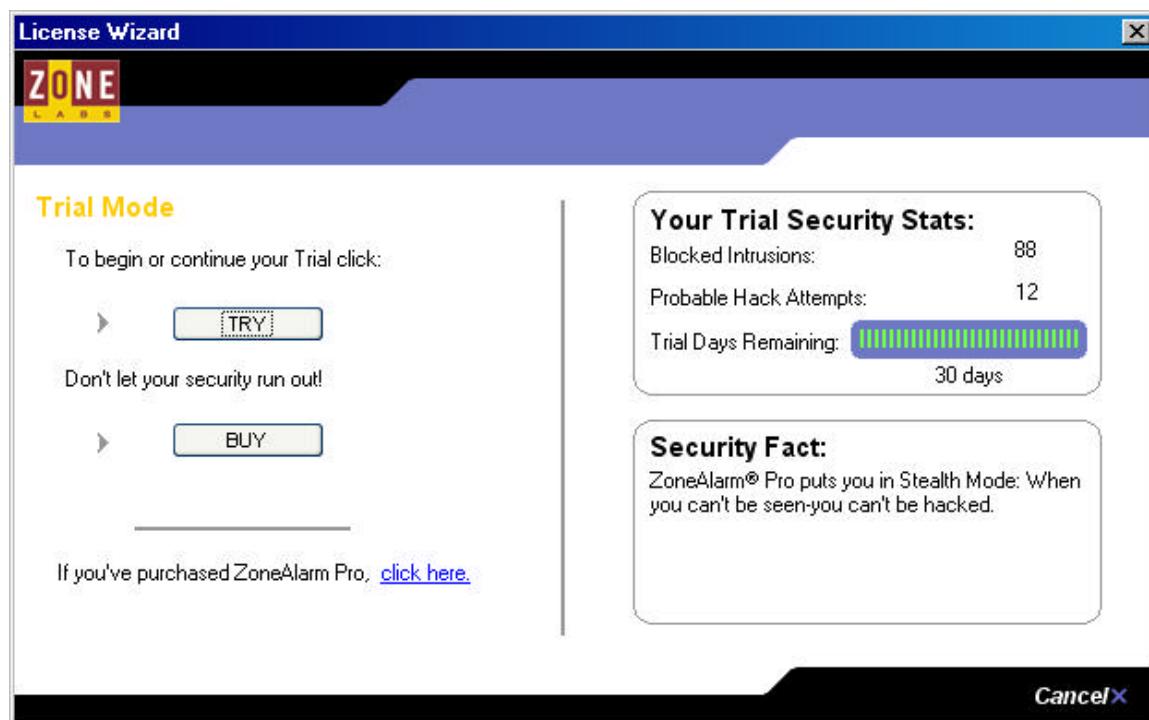
Click **Yes** to start ZoneAlarm Pro immediately.

You see the following notice:



This tells you that ZoneAlarm Pro's True Vector Internet monitor is getting ready to protect you.

Installation screen 6: Try or buy dialog



If you are using a trial license for ZoneAlarm Pro, the “try or buy” dialog appears. The area in the upper right tells you how many trial days remain, and summarize security activity during your trial.

Click **Try** to continue your trial period.

Click **Buy** to purchase ZoneAlarm Pro.

Finally, the Zone Labs logo (ZA) appears in the system tray.

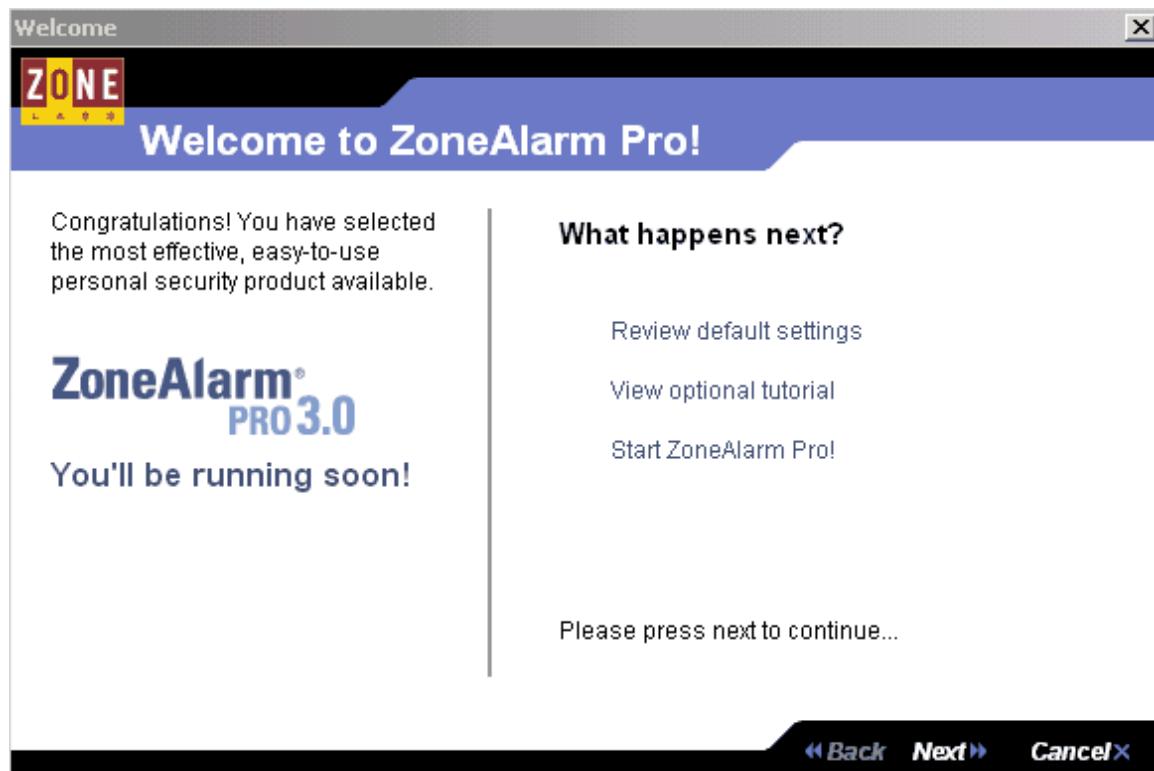
Congratulations! ZoneAlarm Pro is installed!

Configuration Wizard

When installation is complete, ZoneAlarm Pro automatically launches the Configuration Wizard.

The Configuration Wizard helps you quickly and easily set up ZoneAlarm Pro for use in your computing environment.

Configuration Wizard 1: Welcome



The security experts at Zone Labs choose default security settings that are appropriate for most users. Click Next to begin configuration by reviewing default settings for:

- Firewall Alerts
- Cookie Control
- Ad Blocking

Configuration Wizard 2: Review Privacy settings

Configuration Wizard

ZONE
LABS

Review Privacy Settings

 **PRIVACY CONTROL**

ZoneAlarm Pro 3.0 introduces great new privacy controls to block pop-up and pop-under ads along with 3rd-party cookies that can be used to spy on you while you surf the Web.

Would you like to enable ZoneAlarm Pro's privacy control?

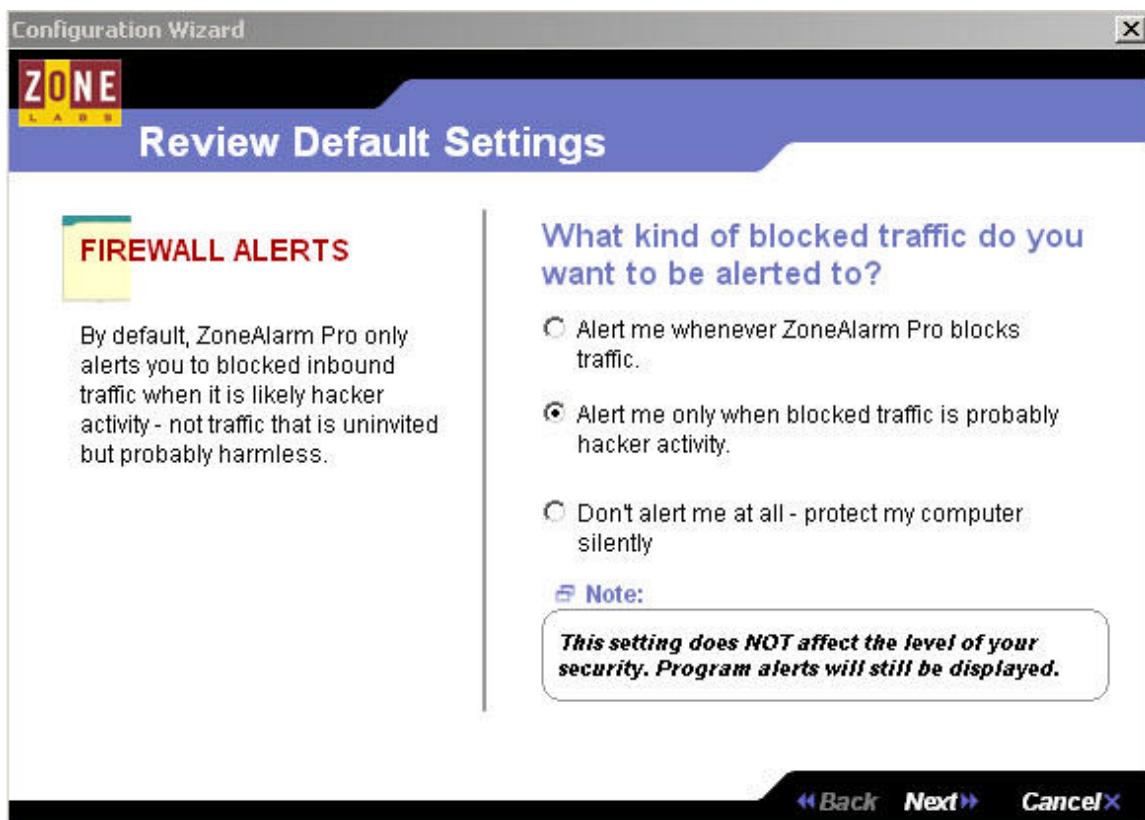
Leave Privacy control off for now. I can always turn it on later in the Privacy panel.

Turn privacy control on so I can block pop-up ads, banner ads and 3rd-party cookies.

« Back **Next »** **Cancel** 

To turn on privacy protection (cookie control, ad blocking, and mobile code control), select the second button, then click **Next**. If you choose not to turn on privacy protection, you can turn it on later using the privacy panel.

Configuration Wizard 3: Review Firewall Alert Settings (Optional)

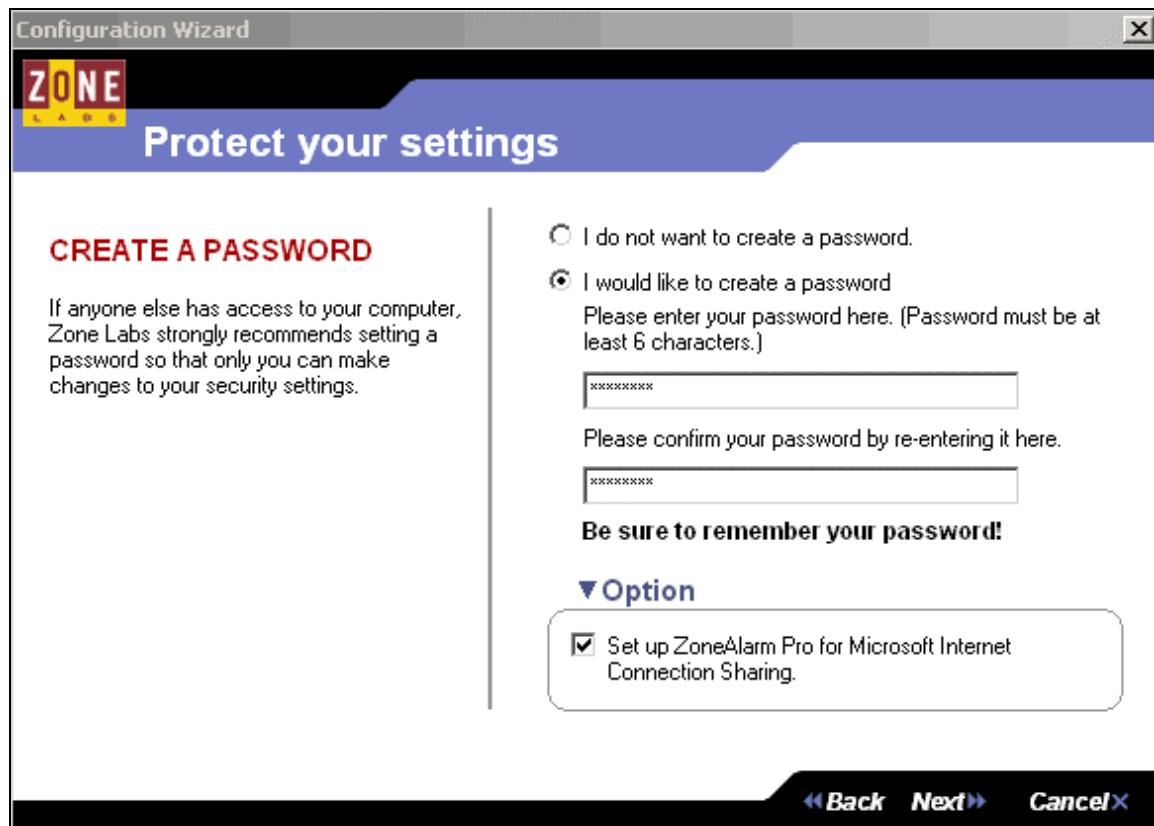


The default Firewall Alert setting is pre-selected. Choose a higher or lower setting, or click **Next** to accept the default.

Choices:

- Alert me whenever ZoneAlarm Pro blocks traffic.**
Choose this setting if you want to be aware of what ZoneAlarm Pro is doing at all times—even when it blocks traffic that is unsolicited, but probably harmless.
- Alert me only when blocked traffic is probably hacker activity.**
This is the default setting. Choose this to be alerted only when there is a potential threat.
- Don't alert me at all – protect my computer silently.**
Choose this if you don't want to be disturbed. ZoneAlarm Pro will protect you without interrupting your work. **Note** that Program alerts will still be displayed, because they require you to grant or deny Internet access to a program.

Configuration Wizard 4: Create a password



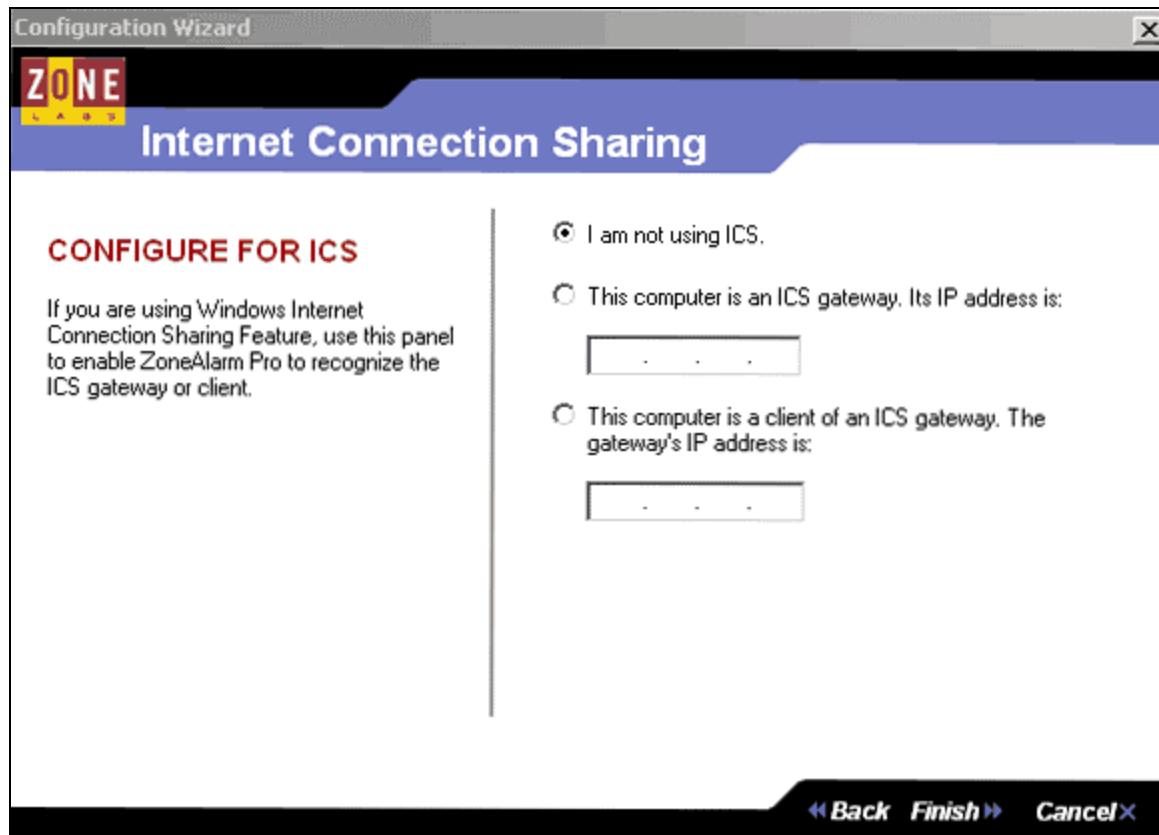
Use this screen to set a password to protect your ZoneAlarm Pro settings. By setting a password, you prevent anyone else from changing your security settings or shutting down ZoneAlarm Pro.

Note Setting a password does not prevent other people from using your computer to access the Internet.

Option

If you are using Microsoft Internet Connection Sharing, select the option check box before clicking **Next**.

Configuration Wizard 5: Configure for ICS

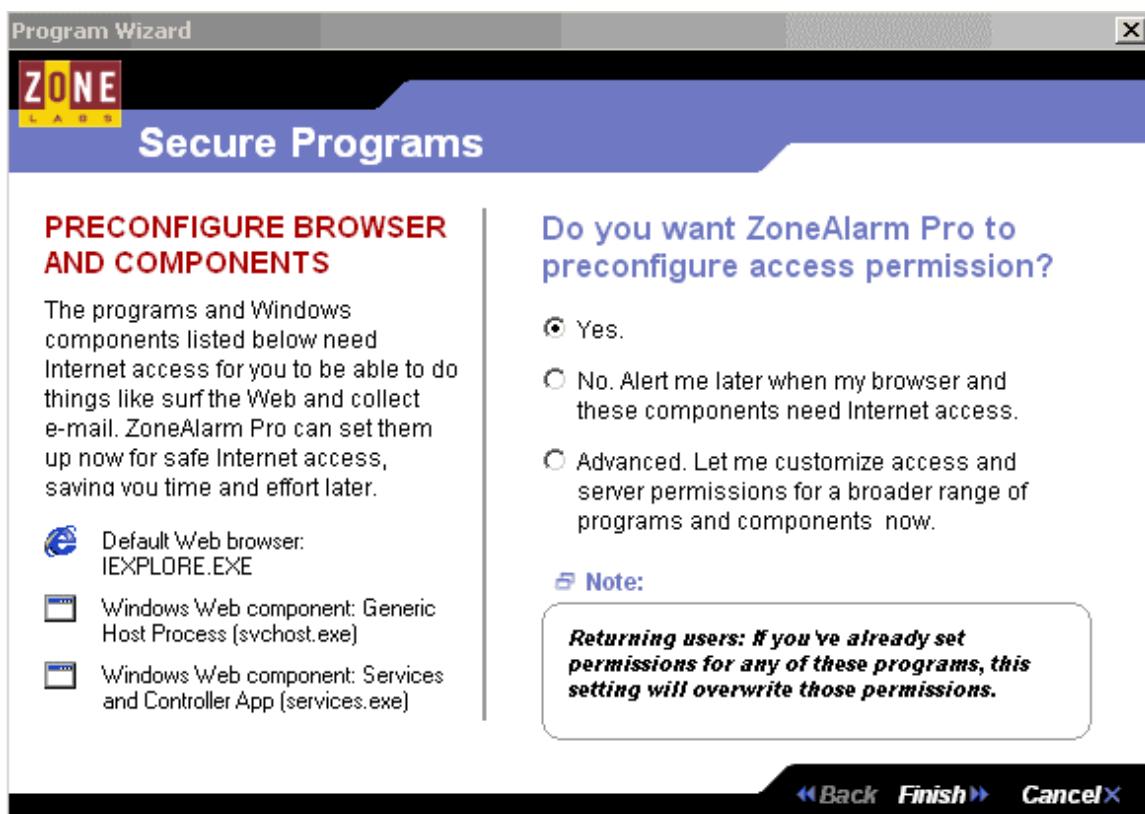


If you are on a local network that uses Windows ICS to share one Internet connection among several computers, you need to configure ZoneAlarm Pro to recognize the ICS gateway/client relationship. Whether ZoneAlarm Pro is installed on the client or the gateway, the ZoneAlarm Pro needs the gateway's IP address.

Choose the gateway or client option, and fill in the IP address.

Click **Finish** to proceed to the next Wizard screen.

Configuration Wizard 6: Preconfigure Browser

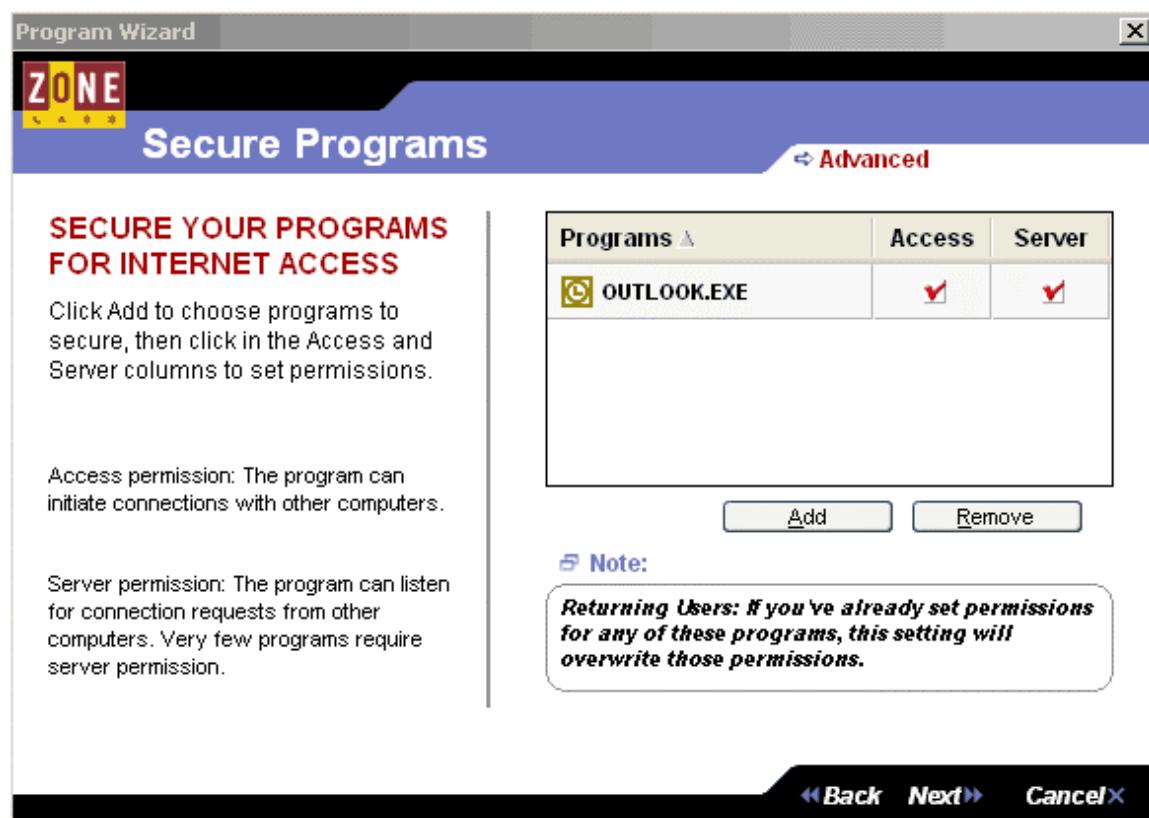


This part of the Wizard enables you to secure your browser and the system components it uses so that they can safely access the Internet.

Choices:

- Yes**
This is the default setting. Choose this to have ZoneAlarm Pro record the MD5 digital signature of your default browser and the system components it uses, and give them Internet access permission. This way, you won't be bothered by a Program Alert later, the first time you open your browser to access the Internet.
- No**
Choose this if you want to wait until the browser requests Internet access, and then give it permission.
- Advanced**
Choose this only if you know what programs you want to give Internet access permission to, and where they are stored on your computer.

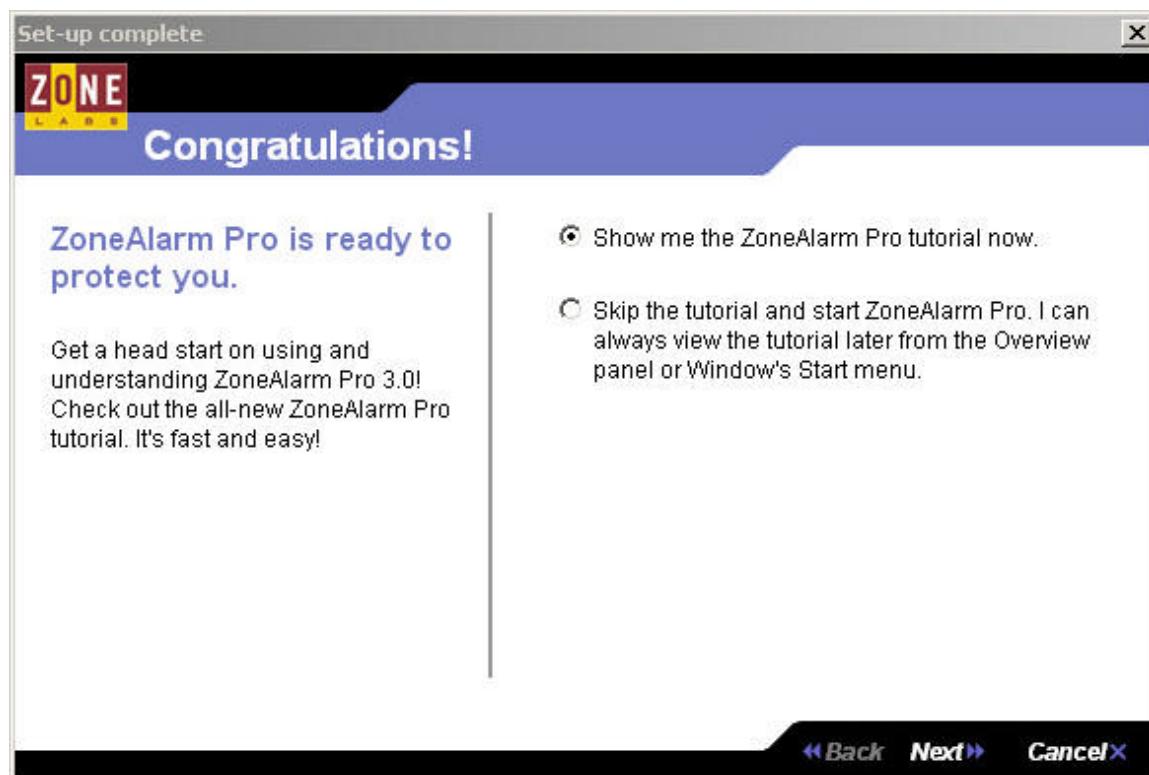
Configuration Wizard 7: Secure Programs



Click **Add** to access the Windows interface and navigate to the programs you want to secure for Internet access. Click the Internet Access and Server Rights columns to give the programs you choose access permission and/or server permission.

Tip For definitions of “access permission” and “server permission” see the glossary.

Configuration Wizard 8: Congratulations!



Your ZoneAlarm Pro configuration is complete. You have the choice of viewing the tutorial in order to get an overview of ZoneAlarm Pro security and alerts.

Choose **Skip the tutorial** to launch ZoneAlarm Pro immediately. You can open the tutorial later from the Status tab.

Your ZoneAlarm Pro configuration is complete!

4 Using ZoneAlarm Pro

Setting up

Your setup may already be complete!

After you have installed ZoneAlarm Pro and run the Configuration Wizard, ZoneAlarm Pro is ready to protect you. You don't have to perform any setup tasks, unless you have special networking or security needs.

Should I change the default security settings?

ZoneAlarm Pro's default settings are appropriate for most Internet users. To learn about the default settings and to find out if they are right for you, see Choosing Security Settings, page 36.

Should I engage the Internet Lock?

No! You don't need to close the Internet Lock except in emergency situations. For more information, see Using the Internet Lock and Stop button, page 54.

How do I know ZoneAlarm Pro is working?

The ZA icon in the lower right corner of your screen tells you ZoneAlarm Pro is protecting you. The icon becomes a red and green traffic indicator whenever network traffic leaves or enters your computer.

What do alerts mean?

If you see alerts, don't panic! Alerts help you configure your Program Control settings, and let you know that ZoneAlarm Pro is protecting you. To find out about the different types of alerts, and to learn how to respond to them, see Responding to Alerts, page 38.

How do I set up for my network?

If you're on a home or business local network, see Networking with ZoneAlarm Pro, page 62.

How do I customize my security?

If you are an expert computer user and you want to take control of the details of your Internet security, see Customizing your Security, page 65.

Choosing Security Settings

Security and convenience

In choosing Internet security settings, your goal is to ensure the highest possible security with the least loss of Internet convenience.

Our security professionals have chosen ZoneAlarm Pro's default security settings with this double goal in mind. They protect your computer from harm and safeguard your information, while keeping your Internet experience convenient.

Example: Cookie control

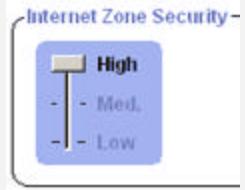
Internet cookies make it possible for e-commerce sites (like Amazon, for example) to recognize you as soon as you arrive and customize the pages you visit to your liking. However, cookies can also be used to record information about your web-surfing habits and give that information to marketers and advertisers.

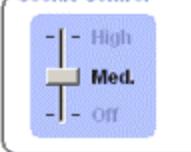
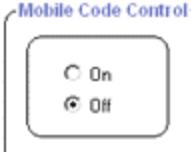
Zone Alarm Pro's default **medium** cookie control setting balances security with convenience by blocking only third-party cookies—those cookies that are used to track your viewing habits. Session cookies and persistent cookies are allowed.

If you wish, you can instantly block all cookies by choosing the **high** cookie-control setting, giving you have full protection against all types of cookie abuse—but at the expense of the convenience that cookies make possible.

ZoneAlarm Pro default settings

For most people, the default settings chosen by the security professionals at Zone Labs provide strong security without sacrificing too much convenience and interactivity.

Control	Default	What the default setting does
Firewall-Internet Zone		Makes your computer invisible to hackers. Traffic to or from the Internet Zone is blocked, unless it is initiated by a program on your computer that you've given permission to communicate with the Internet Zone.

Firewall- Trusted Zone	 <p>Trusted Zone Security</p>	<p>Enables you to share files and printers with computers on your home or local network.</p>
Program Control- Authentication	 <p>Program Control</p>	<p>Programs must ask for permission and be authenticated before communicating with the Internet.</p> <hr/> <p>Note Zone Labs recommends you start with this setting at Medium, and then raise it to High after a few days of normal use. This enables ZoneAlarm Pro to secure your program components without interrupting you unnecessarily.</p>
Alerts & Logs	 <p>Alert Events Shown</p> <ul style="list-style-type: none"> <input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Off 	<p>Only high rated alerts are be shown. This keeps you from being interrupted unnecessarily.</p>
Privacy - Cookies	 <p>Cookie Control</p>	<p>Session cookies and persistent cookies are allowed, but third-party cookies are blocked. This lets you benefit from the convenience of cookies, while preventing advertisers and other third parties from getting information about your Internet habits.</p>
Privacy - Ad blocking	 <p>Ad Blocking</p>	<p>Blocks pop-up ads and banner and skyscraper ads that take more than a few seconds to load. Ads that don't slow down Internet performance are allowed.</p>
Privacy - Mobile Code	 <p>Mobile Code Control</p> <ul style="list-style-type: none"> <input type="radio"/> On <input checked="" type="radio"/> Off 	<p>While mobile code can be a vulnerability, it also is a powerful tool for making Web sites interactive. Mobile code control is turned OFF by default to let you take advantage of that interactivity.</p>

e-mail Protection



Quarantines 37 common types of e-mail attachments, like executable files (.exe) and MS-DOS applications(.com), that can contain worms or viruses.

Tip If you are an expert computer user and you want to take control of the details of your security, see *Customizing your security*, page 65.

Responding to Alerts

When you start using ZoneAlarm Pro, you may see several types of alerts. Don't worry! Alerts don't necessarily mean you are under attack, and they can help you configure your security.

ZoneAlarm Pro alerts fall into two categories:

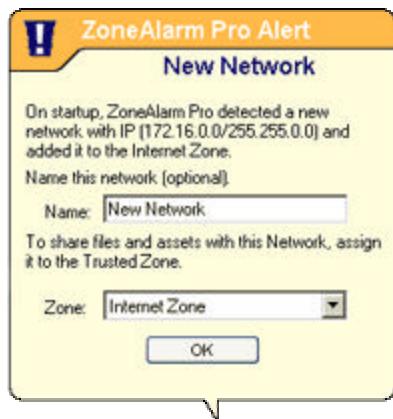
- **Informational** alerts let you know that ZoneAlarm Pro has protected you by blocking a communication that didn't fit your security rules. By clicking **OK**, you're not allowing anything into your computer—you're just saying "yes, I've seen the alert."
- **Query** alerts ask you if you want to allow something to happen, offering you a **Yes** or **No** choice.

The alerts you're likely to see most often are these:

- **New Network alerts.** These are informational. However, They also give you the opportunity to add a new network to your Trusted Zone.
- **Firewall alerts.** These are informational.
- **New Program alerts.** These are query alerts. They ask you whether to allow a program Internet access or server access.

This chapter tells you how to respond to these common alerts and other alerts you may also see when using ZoneAlarm Pro.

New Network alerts



If you're on a home or local network, New Network alerts let you instantly configure ZoneAlarm Pro to allow you to share resources with the network.

Why these alerts occur

New Network alerts occur when you connect to any new network--be it a wireless home network, a business LAN, or your ISP's network.

What you should do

If you receive a New Network alert when you start ZoneAlarm Pro, and you are connected to a home or business local network, it is likely that ZoneAlarm Pro has detected that network.

If you want to share resources with the other computers on the network, put the network in the Trusted Zone by following the steps below:

5. In the New Network alert pop-up, type a name for the network (for example "Home NW") in the Name box.
6. Select **Trusted Zone** from the Zone drop-down list.
7. Click **OK**.

Caution If you are not certain what network ZoneAlarm Pro has detected, write down the IP address displayed in the alert box. Then consult your home network documentation, systems administrator, or ISP to determine what network it is.

If you are connected to the Internet through a standard modem and dial-up connection, a Digital Subscriber Line (DSL), or a cable modem, it is likely that ZoneAlarm Pro has detected your ISP's network.

To secure your Internet connection, click **OK** in the New Network alert pop-up.

Caution If you click **Cancel**, ZoneAlarm Pro will block your Internet connection. Do not add your ISP network to your Trusted Zone.

About wireless networks

Use caution if ZoneAlarm Pro detects a wireless network. It is possible for your wireless network adapter to pick up a network other than your own. Be sure that the IP address displayed in the New Network alert is your network's IP address before you add it to the Trusted Zone.

How you can see fewer of these alerts

It is unusual to receive a lot of New Network alerts.

New Program alerts



New Program alerts are central to your Internet security. They ensure that no program on your computer can use your Internet connection without your permission, preventing hackers from communicating with Trojan horses or other malware they may have distributed. They enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before. If you click **Yes**, the program is allowed access. If you click **No**, the program is denied access.

Why these alerts occur

New Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has not already received access permission from you.

There are many programs and program components that require access permission as part of their normal function. Browsers and e-mail client applications, for example, must connect to remote servers to retrieve Web pages and send or receive e-mail.

Most of the time, you're likely to see program alerts when you're actually using a program. For example, if you've just installed ZoneAlarm Pro, and you immediately open Microsoft Outlook and try to send an e-mail message, you'll get a program alert asking if you want Outlook to have Internet access.

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

8. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click **Yes**. If not, continue with step 2.
9. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click **Yes**. If not, or if you're not sure, continue with step 3.
10. Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer **Yes**.

Tip If you're really not sure what to do, it's best to answer **No**. You can always grant permission later by going to the Programs tab.

How you can see fewer of these alerts

It's normal to see several New Program alerts soon after installing ZoneAlarm Pro. As you assign permissions to each new program, the number of alerts you see will decrease.

Tip To avoid seeing Repeat Program alerts, select **Remember this answer the next time I use this program** before clicking **Yes** or **No**.

Firewall alerts



When you see a Firewall alert, it means that ZoneAlarm Pro has protected you by blocking traffic not allowed by your Firewall settings. By clicking **OK**, you are not letting anything into your computer--you are only saying "**Yes**, I've seen the alert."

Why these alerts occur

Firewall alerts occur when ZoneAlarm Pro blocks an incoming or outgoing packet because of the port and protocol restrictions set in the Firewall panel.

Firewall alerts can be caused by harmless network traffic, for example, if your ISP is using ping to verify that you're still connected. However, they can also be caused by a hacker trying to find unprotected ports on your computer.

If the alert was probably caused by harmless network traffic, the alert has an orange band at the top. If the alert was probably caused by hacker activity, the pop-up has a red band at the top

What you should do

When you see a Firewall alert, there's nothing you have to do to ensure your security.

To dismiss the alert box, click **OK**. By doing this, you're not allowing any traffic in or out of your computer.

If you're interested in learning more about the alert, for example, the common uses of the port it was addressed to, or the likelihood that it stemmed from hacker activity, click the **More Info** button. This submits your alert information to Zone Labs' AlertAdvisor, which analyzes the information and provides the most likely explanation.

How you can see fewer of these alerts

If you are receiving a lot of firewall alerts, but you don't suspect you're under attack:

Make sure your Trusted Zone security is set to medium

If you're on a home or business network, and your Trusted Zone security is set to high, normal LAN traffic such as NetBIOS broadcasts may generate firewall alerts. Try lowering Trusted Zone security to medium.

Determine if the source of the alerts should be trusted

Repeated alerts may indicate that a resource you want to trust is trying repeatedly to contact you.

11. Submit repeated alerts to AlertAdvisor, by clicking the **More Info** button in the Log Viewer tab. See page 106.
12. Use AlertAdvisor to determine whom the source IP address that caused the alerts belongs to.
13. If the alerts were caused by a source you want to trust, add it to the Trusted Zone. Do this in the Log Viewer tab. See page 106.

Determine if your Internet Service Provider is sending you "heartbeat" messages

Try the procedures suggested for managing ISP heartbeat. [See ISP heartbeat](#), page 64.

Set your alert display controls to medium

By default, ZoneAlarm Pro only displays high-rated firewall alerts. If your defaults have been changed, you may see a lot of medium-rated alerts. Try setting your alert display settings to medium, in the Main tab of the Alerts & Logs panel. See page 105.

Other alerts

Repeat Program alert



If you respond **Yes** or **No** to a program alert without checking Remember this answer the next time I use this program, you'll see a Repeat Program alert the next time the program asks for access permission.

Why these alerts occur

Repeat Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has asked for permission before.

There are many programs and program components that require access permission as part of their normal function. Browsers and e-mail client applications, for example, must connect to remote servers to retrieve Web pages and send or receive e-mail.

Most of the time, you will see program alerts when you're actually using a program. For example, if you've just installed ZoneAlarm Pro, and you immediately open Microsoft Outlook and try to send an e-mail message, you'll get a program alert asking if you want Outlook to have Internet access.

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

14. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click **Yes**. If not, continue with step 2.
15. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click **Yes**. If not, or if you're not sure, continue with step 3.
16. Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and

the program. Use the AlertAdvisor information to help you decide if it's safe to answer **Yes**.

Tip If you're really not sure what to do, it's best to answer **No**. You can always grant permission later by going to the Programs tab. See page 92.

How you can see fewer of these alerts

To keep from seeing Repeat Program alerts, select **Remember this answer the next time I use this program** before clicking **Yes** or **No** in any New or Repeat program alert. This sets the permission for the program to Allow or Block in the Programs tab.

Server Program alert



Server Program alerts enable you to set server permission for a program on your computer. See also *Server Permission*, page 135.

Why these alerts occur

Server Program alerts occur when a program on your computer wants server permission for either the Internet Zone or Trusted Zone, and that program has not already received permanent server permission from you.

Relatively few programs on your computer will require server permission. Some common types of programs that do are:

- Chat
- Internet Call Waiting
- Music file sharing (such as Napster)
- Streaming Media (such as RealPlayer)
- Voice-over-Internet
- Web meeting

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

1. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click **Yes**. If not, continue with step 2.
2. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click **Yes**. If not, or if you're not sure, continue with step 3.
3. Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer **Yes**.

Caution If you are still not certain that the program is legitimate and needs server permission, it is safest to answer **No**. If it becomes necessary, you can give the program server permission later by using the Programs tab.

How you can see fewer of these alerts

If you are using the types of programs described above that require server permission to operate properly, use the Programs tab in ZoneAlarm Pro to grant permission before you start using the program. See also *Programs tab*, page 92.

Changed Program alert



Why these alerts occur

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow and is asking for permission again. If you click **Yes**, the changed program is allowed access. If you click **No**, the program is denied access.

Changed Program alerts can occur if you have updated a program since the last time it accessed the Internet. However, they can also occur if a hacker has somehow managed to tamper with the program.

What you should do

Click **Yes** or **No** in the alert pop-up after asking these questions:

- Did you (or, if you're in a business environment, your systems administrator) recently upgrade the program that is asking for permission?
- Does it make sense for the program to need permission?

If you can answer "yes" to both question, it's probably safe to click **Yes**.

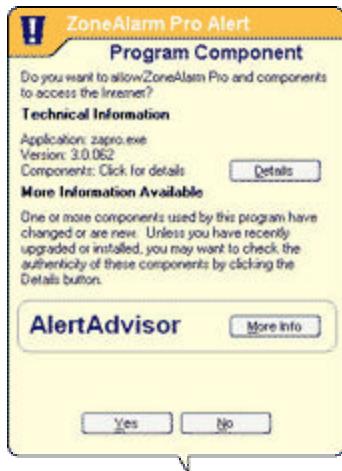
Tip If you're not sure, it's safest to answer **No**. You can always grant permission later in the Programs tab. See *Programs tab*, page 92.

If you're not sure what to do, or if you decide to answer **No**, investigate the program to determine if it is safe. See *Investigating changed programs and components*, page 53.

How you can see fewer of these alerts

To avoid a large number of Changed Program alerts, avoid unnecessary or repeated program updates.

Program Component alert



Use the Program Component alert to allow or deny Internet access to a program that is using one or components that haven't yet been secured by ZoneAlarm Pro. This helps protect you from hackers who try to use altered or faked components to get around your program control restrictions.

By clicking **Yes**, you allow the program to access the Internet while using the new or changed components. By clicking **No**, you prevent the program from accessing the Internet while using those components.

Click the **Details** button to see what component(s) the program was

Why these alerts occur

Program Component alerts occur when a program accessing the Internet or local network is using one or more components that ZoneAlarm Pro has not yet secured, or that has changed since it was secured.

Note ZoneAlarm Pro automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser.

What you should do

The proper response to a Program, Component alert depends on your situation. Consider the following questions:

1. Are any of the following true?

- You just installed or reinstalled ZoneAlarm Pro.
- You recently updated the application that is loading the component (For the application name, look under Technical Information in the alert pop-up.)
- The application that is loading the component has an automatic update function.
- Someone else (for example, a systems administrator at your workplace) may have updated a program on your computer without your knowledge.

2. Are you actively using the application that loaded the component?

If you can answer "yes" to both questions, it is likely that ZoneAlarm Pro has detected legitimate components that your browser or other programs need to use. It is probably safe to answer **Yes** to the Program Component alert.

If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to answer **No**.

If you're not sure what to do, or if you decide to answer **No**, investigate the component to determine if it is safe. See *Investigating changed programs and components*, page 53.

How you can see fewer of these alerts

You may receive a large number of component alerts if you raised the Program Authentication level to high soon after installing ZoneAlarm Pro. With authentication set to High, ZoneAlarm Pro cannot automatically secure the large number of DLLs and other components commonly used by browsers and other programs.

To greatly reduce the number of alerts, lower the Program Control level to medium for the first few days after installing ZoneAlarm Pro. See *Main tab (Program Control panel)*, page 90.

If you have been using ZoneAlarm Pro for more than a few days, it is very rare to see large numbers of program alerts.

Component Loading alert



Use the Component Loading alert to allow or deny Internet access to program that is loading a new or changed component some time after the program was launched. This helps protect you from hackers who try to use altered or faked components to get around your program control restrictions.

By clicking **Yes**, you allow the program to continue to access the Internet or local network resources while using the new or changed component. By clicking **No**, you prevent the program from accessing the Internet while using that component.

Tip Click the **Details** button to see what component(s) the program was loading

Why these alerts occur

A Component Loading alert can occur in several normal situations. For example, if you click a link to a .pdf document, and your browser has not yet loaded the components necessary to read .pdf files, you will see a Component Loading alert as the browser loads those components.

However, a Component Loading alert can also occur if someone has tampered with a component, or created a malicious component designed to use a known program as a resource.

Component Loading alerts occur when all of the following are true:

- The Program Control level is set to **High**.
- A repeat program (one that has requested Internet access before, and whose MD5 signature has been recorded by ZoneAlarm Pro) loads a new component some time after the program itself has loaded.

- That component is new or has changed, or has **Ask** permission set in the Components tab.

What you should do

The proper response to a Component Loading alert depends on your situation. Consider the following questions:

- Are you actively using the application that loaded the component?
- If the program that loaded the component was your browser, did you just try to access functionality that might require the browser to load a new component? Some examples of such functionality are flash videos and .pdf files.

If you can answer "**Yes**" to both questions, it is likely that ZoneAlarm Pro has detected legitimate components that your browser or other programs need to use. It is probably safe to answer **Yes** to the Component Loading alert.

If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to answer **No**.

How you can see fewer of these alerts

It is unusual to see a large number of Component Loading alerts. However, you may receive a large number of alerts if you raised the Program Authentication level to high soon after installing ZoneAlarm Pro. With authentication set to High, ZoneAlarm Pro cannot automatically secure the large number of DLLs and other components commonly used by browsers and other programs.

To greatly reduce the number of alerts, lower the authentication level to medium for the first few days after installing ZoneAlarm Pro

If you're not sure what to do, or if you decide to answer **No**, investigate the component to determine if it is safe. See *Investigating changed programs and components*, page 53.

MailSafe alert



MailSafe alerts let you know that ZoneAlarm Pro has quarantined a potentially dangerous attachment to an incoming e-mail message. By clicking **Yes**, you're not letting anything into your computer.

Why these alerts occur

MailSafe alerts occur when you open an e-mail that has an attachment whose filename extension is on the list of extensions to be quarantined in the MailSafe panel. The alert informs you that ZoneAlarm Pro has changed the extension to prevent the attachment from being opened without warning.

About e-mail borne viruses and worms

E-mail messages are the most common way Internet viruses and worms are spread. Some worms can raid your e-mail address book and forward themselves to everyone in it. When your friends see the message, they'll think it came from you, and open it--thus repeating the cycle.

For best security, you should never open an e-mail attachment that ZoneAlarm Pro has quarantined without first confirming the following three things:

- That it actually came from someone you know and trust
- That that person sent it intentionally
- That that person is sure that the attachment is harmless

What you should do

Click **OK** to close the alert box, then follow the steps below to ensure your security.

1. Examine the e-mail message carefully. Are you sure it's from someone you know and trust? Remember, hackers can fake e-mail messages so that they look like they are from a friend. Also, if a friend has accidentally opened a file containing an e-mail worm, that worm may have sent itself to you, using your friend's e-mail program.
2. If you're not completely sure the message is genuine, contact the sender by telephone or e-mail before trying to open the attachment.
3. If you're certain the attachment is harmless, you can open it by clicking the quarantine icon (which replaces the normal file icon).

Tip When you try to open a quarantined attachment, ZoneAlarm Pro will display a warning dialog box to remind you that the attachment is potentially dangerous.

How you can see fewer of these alerts

It is extremely unusual to receive a large number of MailSafe alerts, unless you regularly receive e-mail with executable files attached. If you frequently receive executable attachments from trusted correspondents, have those correspondents compress the attachments into .zip files before sending.

Internet Lock alerts



Internet Lock alerts let you know that ZoneAlarm Pro has blocked incoming or outgoing traffic because the Internet Lock (or the Emergency Lock) is engaged. By clicking **Yes**, you're not opening the lock; you're just acknowledging that you've seen the alert.

Why these alerts occur

These alerts occur only when the Internet Lock is engaged.

To learn more about the Internet Lock, see *Using the Internet Lock and Stop button*, page 54.

What you should do

Click **OK** to close the alert pop-up.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts.

Tip You may want to give certain programs (for example, your browser) permission to bypass the Internet Lock, so that you can continue to perform some basic functions under the lock's higher security. See *Programs tab*, page 92.

How you can see fewer of these alerts

If you are receiving a lot of Internet Lock alerts, it is possible that your Automatic Internet Lock settings are engaging the Internet Lock after every brief period of inactivity.

To reduce the number of alerts, you can do any of the following:

- In the Programs tab, turn the Automatic Internet Lock off.
- In the Auto-Lock tab, increase the number of minutes of inactivity required for the Automatic Lock to engage.

See also *Programs tab*, page 92 and *Auto-Lock tab*, page 98.

Blocked Program alerts



Blocked Program alerts tell you that ZoneAlarm Pro has prevented an application on your computer from accessing the Internet or Trusted Zone resources. By clicking **OK**, you're not allowing the program access, just acknowledging that you saw the alert.

Why these alerts occur

Blocked Program alerts occur when a program tries to access the Internet or the Trusted Zone, even though you have explicitly denied it permission to do so. Because you've already configured ZoneAlarm Pro to block the program, the alert displays only an **OK** button, rather than the **Yes** and **No** options that appear in other Program alerts.

What you should do

Click **OK** to close the alert pop-up. There's nothing further you have to do to ensure your security.

If the program that was blocked is one that you want to have access to the Internet Zone or Trusted Zone, use the Programs tab to give the program access permission. See *Programs tab*, page 92.

How you can see fewer of these alerts

To turn off Blocked Program alerts, do either of the following:

- When you see a Blocked Program alert, select **Do not show this dialog again** before clicking **OK**. From then on, all Blocked Program alerts will be hidden. **Note** that this will not affect New Program, Repeat Program, or Server Program alerts.
- In the Program Control panel, click **Advanced** to access the Alerts & Functionality tab, then clear the check box labeled **Show alert when Internet access is denied**.

Note Turning off Blocked Program alerts does not affect your level of security.

Investigating changed programs and components

When you receive a Changed Program alert, a Program Component alert, or a Component Loading alert, you may want to investigate to see if there is a known hacker exploit or other problem associated with the program or component that caused the alert.

Investigating changed programs

Use virus scanning/Trojan scanning software and technical support resources to determine if a changed program is dangerous or not.

Tip In order to investigate the program, you will need the file name, version number, and location of the file on your computer. You can get this information from the Changed Program alert box.

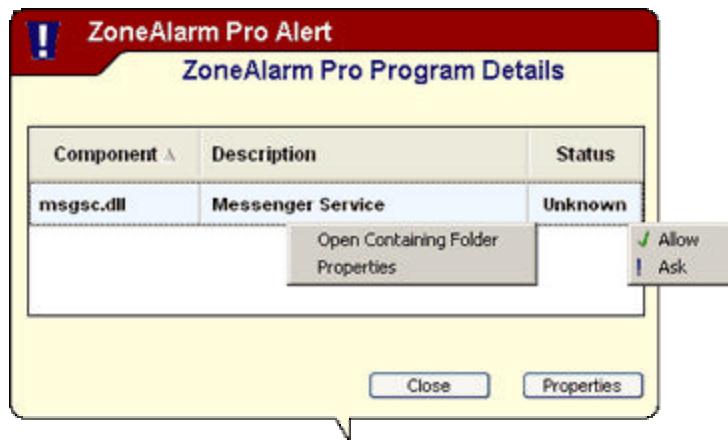
Follow these steps to investigate the program:

1. Make sure your virus scanner/Trojan scanner is up to date
2. Scan the program file.
3. If your scanner does not indicate a virus or other problem, contact the technical support staff of the manufacturer of the changed program. They may be able to give a reason why the program changed, such as an automatic update.

Investigating changed components

When you receive a Program Component alert or Component Loading alert, It can be difficult to determine if the component is dangerous or not.

Tip In order to investigate the component, you will need the file name, version number, and location of the file on your computer. You can get this information from the Program Component alert box, and from the Program Details box, shown below.



Access the Program Details box by clicking the **Details** button in a Program Component alert or Component Loading alert. To view the properties of the component, click the description, then choose **Properties** from the shortcut menu. To view the Windows directory that the component is located in, click the description, then choose **Open containing folder** from the shortcut menu.

Follow these steps to investigate the component:

1. Go to the Microsoft support site (<http://support.microsoft.com>), and search the knowledgebase using the file name and description of the component as search terms.
2. Contact the technical support staff of the manufacturer of the program that loaded the changed component. They may be able to tell you why the component changed.
3. Perform an Internet search, using the file name of the component as a search term. We suggest using the Google search engine.

Using the Internet Lock and Stop button

The Stop button enables you to instantly "shut the doors" to your computer if you think you are under attack, while the Internet Lock offers extra protection when you leave your computer unattended for a time. The lock can be activated manually or automatically.

What's the difference between Stop and Lock?



The Stop button stops ALL traffic to and from your computer--no exceptions!

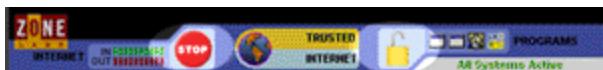
The Internet Lock stops all traffic to and from your computer, EXCEPT traffic initiated by programs to which you have given pass-lock permission. These programs can continue to communicate normally even when the lock is engaged. For a definition of pass-lock permission see the *Glossary*, page 125.

In the Programs tab, a lock icon indicates that the program has pass-lock permission. Click the icon to remove permission.

Program Control		Main	Programs
Active	Programs ▾	Access	
		Trusted	Internet
	Internet Explorer	Off	✓ ✓
✓	LSA Executable and	✓	■

Turning the lock on and off

There are two ways to manually activate or deactivate the Internet Lock and Stop functions:



Click the **Stop** button or the Lock icon on the dashboard



Select from the pop-up system tray menu.

In addition, the Internet Lock can be activated automatically.

How do I know the Lock is on?

If the **Stop** button has been clicked, you'll see a red lock icon in the system tray. You may also begin to see a lot of alerts.



If the Internet **Lock** has been clicked, you'll see a yellow lock icon.



To turn either function off, just click the icon again.

Using the Automatic Internet Lock

The Automatic Internet Lock protects your computer if you leave it connected to the Internet for long periods even when you're not actively using network or Internet resources.

When enabled, the automatic lock engages:

- When your screensaver engages, or
- After a specified number of minutes of network inactivity.

You can turn the automatic lock on or off in the Programs tab. For more information about customizing automatic lock settings, see *Auto-Lock tab*, page 98.

Using your programs with ZoneAlarm Pro

Anti-virus software

Automatic updates

In order to receive automatic updates from your anti-virus software vendor, add the domain that contains the updates (e.g. update.avsupdate.com) to your Trusted Zone.

See *Zones tab*, page 82.

E-mail protection

In some cases, ZoneAlarm Pro's MailSafe feature may conflict with the e-mail protection features of anti-virus software. If this occurs, you can adjust ZoneAlarm Pro and anti-virus settings so that you benefit from both anti-virus and ZoneAlarm Pro protection. Follow these steps:

1. Set your anti-virus program to scan all files on access, and disable the e-mail scanning option.
2. In ZoneAlarm Pro, enable MailSafe.
3. In the Alert Events tab (accessed by clicking the **Advanced** button in the Alerts & Logs Overview tab), turn off alert display for quarantined MailSafe attachments.

With this configuration, MailSafe will still quarantine suspect e-mail attachments, and warn you when you try to open them. If you elect to open an attachment anyway, your anti-virus software will still scan it.

Browsers

In order for your browser to work properly, it must have access permission for the Internet Zone and Trusted Zone. You can grant access in any of the following ways:

- Run the Program Wizard from the Overview tab of the Program Control panel. ZoneAlarm Pro will automatically detect your default browser and prompt you to grant it Internet Zone access.
- Go to the Programs tab in the Program Control panel, and use the controls there to grant access.
- Answer **Yes** when a Program alert for the browser appears.

See also *Programs tab*, page 92.

Windows 2000

If you are using Windows 2000, you may need to allow Internet access rights to the Services and Controller App (the file name is typically services.exe). To do this:

1. Open the Programs tab in the Program Control panel.
2. Locate Services and Controller App in the program list.
3. Click the buttons in the Access field, and select Allow from the pop-up menu.

Netscape

Netscape Navigator versions above 4.73 will typically experience no problems running concurrently with ZoneAlarm Pro . If you are using Navigator version 4.73 or higher are still experiencing difficulty accessing the web with ZoneAlarm Pro active, check the browser Preferences to make sure you are not configured for proxy access.

Tip Make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

Chat/Instant Messaging

Chat and instant messaging programs (for example, AOL Instant Messenger and ICQ) may require server permission in order to operate properly. You can grant server permission by:

- Answering "Yes" to the Server Program alert caused by the program, or
- Using the Programs tab.

For more information see *Server Program alert*, page 44, and *Programs tab*, page 92.

Caution We strongly recommend that you set your chat software to refuse file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, and Trojan horses. Refer to your chat software vendor's help files to learn how to configure your program for maximize security.

Tip For best security, we suggest that mIRC users disable the IDENT function in the mIRC interface.

E-mail programs (e.g., MS Outlook)

In order for your e-mail program (for example, Microsoft Outlook) to send and receive mail, it must have access permission for the Zone the mail server is in. In addition, some e-mail client software may have more than one component requiring server permission.

For example, MS Outlook requires both the base application (OUTLOOK.EXE) and the Messaging Subsystem Spooler (MAPISP32.exe) to have server permission.

While you can give your e-mail program access to the Internet Zone, and leave the mail server there, it's safer to place the mail server in the Trusted Zone, and limit the program's access to that Zone only. Once your e-mail client has access to the Trusted Zone, add the remote mail server (host) to the Trusted Zone.

Use the Programs tab to grant access and server permission.

Use the Zones tab to place servers in the Trusted Zone.

File Sharing

File sharing programs, such as Napster, Limewire, AudioGalaxy, or any Gnutella client software, must have server permission for the Internet Zone in order to work with ZoneAlarm Pro.

Use the Programs tab to grant access and server permission.

FTP

To use FTP (File Transfer Protocol) programs, you may need to make the following settings adjustments in your FTP client program and in ZoneAlarm Pro.

- Enable passive or PASV mode in your FTP client

This tells the client to use the same port for communication both directions. If PASV is not enabled, ZoneAlarm Pro may block the FTP server's attempt to contact a new port for data transfer.

- Add the FTP sites you use to the Trusted Zone
- Give Trusted Zone access permission to your FTP client program.

Use the Programs tab to grant access and server permission.

Use the Zones tab to place servers in the Trusted Zone.

Games

In order to play games over the Internet while using ZoneAlarm Pro, you may have to adjust the following settings.

Program permission

For an Internet game to function properly, it will require Internet access and/or server permission.

The easiest way to grant access is to answer "Yes" to the program alert caused by the game program. However, Many games run in "exclusive" full screen mode, which will prevent you from seeing the alert. Use any of the methods below to solve this problem.

- Set the game to run in a window

This will allow you to see the alert, if the game is running at a resolution lower than that of your desktop. If the alert appears but you respond to it because your mouse is locked to the game, press the Windows logo key on your keyboard.

After granting the game program Internet access, reset the game to run full-screen.

- Use software rendering mode

By changing your rendering mode to "Software Rendering," you can allow Windows to display the ZoneAlarm Alert on top of your game screen. After allowing the game Internet access, you can change back to your preferred rendering device.

- Use Alt+Tab

Press Alt+Tab to toggle back into Windows. This leaves the game running, but allows you to respond to the alert. Once you have allowed Internet access, press Alt+Tab again to restore your game.

Note This may cause some applications to crash, especially if you are using Glide or OpenGL; however, the problem should be corrected the next time you run the game. Sometimes you can use Alt-Enter in the place of Alt-Tab.

Use the Programs tab to grant access and server permission.

Security level/Zone

Some Internet games, particularly those that use java, applets, or other web-based portal functionality, may not work properly when your Internet security level is set to **high**. High security will also prevent remote game servers from "seeing" your computer. To solve these problems, you can:

- Change your Internet Zone security level to medium, or
- Add the game server you're connecting to to your Trusted Zone. The game documentation or from the game manufacturer's Web site should indicate the IP address or host name of the server.

Use the Zones tab to place servers in the Trusted Zone.

Caution Trusting game servers means trusting the other players in the game. ZoneAlarm Pro does not protect you from attacks instigated by fellow gamers in a trusted environment. Make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

Firewall settings

ZoneAlarm Pro dynamically opens and closes ports as needed when you're gaming, so no adjustments to firewall configuration need to be made.

Internet call waiting/ Internet answering machines

To use Internet answering machine programs (such as CallWave) with ZoneAlarm Pro, do the following:

1. Give the program access permission and sever permission for the Internet Zone.
2. Add the IP address of the vendor's servers to the Trusted Zone.
3. Set the security level for the Internet Zone to medium.

Tip To find the server IP address, contact the vendor's technical support.

Use the Zones tab to place servers in the Trusted Zone.

Remote control and display

PCAnywhere and Timbuktu

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu:

1. Add the IP address(es) of the hosts or clients to which you connect to your Trusted Zone.
2. Add the subnet of the network you are accessing remotely to your Trusted Zone.
3. If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.

Use the Zones tab to place subnets in the Trusted Zone.

Note If your remote control client or host is on a network not under your control (for example on a business or university LAN), perimeter firewalls or other features of the network may prevent you from connecting. If you still have problems connecting after following the instructions above, contact your network administrator for assistance.

VNC

In order for VNC and ZoneAlarm Pro to work together, follow the steps below.

1. On the server machine, do one of the following:
 - If you know the IP address or subnet of the viewer (client) you will be using for remote access, and it will always be the same, add that IP or subnet to the Trusted Zone. This is the preferred option.
 - If you do not know the IP address of the viewer, or it will change, then give the program access permission and server permission for the Trusted and Internet Zones.
2. On the viewer (client) machine, run VNCviewer to connect to the server machine. Do not run in "listen mode."
3. On the viewer (client) machine, do one of the following:
 - If you know the IP address or subnet of the server, and it will always be the same, add that address or subnet to the Trusted Zone. This is the preferred option.
 - If you do not know the IP of the Server, or it will change, then give the program access permission and server permission for both the Trusted Zone and Internet Zone.
4. When prompted by VNCviewer on the viewer machine, enter the name or IP address of the server machine, followed by the password when prompted. You should be able to connect.

Caution If you enable VNC access by giving it server permission and access permission, be sure to **set and use your VNC password** in order to maintain security. We recommend adding the server and viewer IP addresses to the Trusted Zone, rather than giving the application Internet Zone permission, if possible.

Tip Leave the Trusted Zone security level on medium. If you raise it to high, you may have access problems.

Use the Zones tab to place servers in the Trusted Zone.

Use the Programs tab to grant access and server permission.

Telnet

To access a remote server via Telnet, add the IP address of that server to your Trusted Zone.

Streaming audio/video

Applications that stream audio and video, such as RealPlayer, Windows Media Player, QuickTime, and so forth, etc. must have server permission for the Internet Zone in order to work with ZoneAlarm Pro.

Voice over IP (VoIP)

To use Voice over IP (VoIP) programs with ZoneAlarm Pro, you will have to do one or both of the following, depending on the program:

1. Give the VoIP application server permission and access permission.
2. Add the VoIP provider's servers to the Trusted Zone. To learn the IP addresses of these servers, contact your VoIP provider's customer support.

Networking with ZoneAlarm Pro

Making your computer visible on your local network

If you can't see the other computers on your local network, or they can't see you, it is possible that ZoneAlarm Pro is blocking NetBIOS traffic necessary for Windows network visibility.

To make your computer visible to the others on your local network:

1. In the Zones tab of the Firewall panel, add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone.
2. In the Main tab of the Firewall panel, set the Trusted Zone security level to medium, and the Internet Zone security level to high. This allows trusted computers to access your shared files, but blocks all other machines from accessing them.

Note ZoneAlarm Pro will detect your network automatically and display the New Network alert. You can use the alert itself to add your network subnet to the Trusted Zone. See also *New Network alert*, page 39.

Sharing files and printers across a local network

ZoneAlarm Pro enables you to quickly and easily secure your computer so that the trusted machines you're networked with can access your shared resources, but Internet intruders can't use your shares to compromise your system.

To configure ZoneAlarm Pro for secure sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone.
2. Set the Trusted Zone security level to medium. This allows trusted computers to access your shared files.
3. Set Internet Zone security level to high. This makes your computer invisible to non-trusted machines.

Note ZoneAlarm Pro will detect your network automatically and display the New Network alert. You can use the alert itself to add your network subnet to the Trusted Zone. For more information see *New Network alert*, page 39.

VPN (Virtual Private Network)

If you run a VPN client, ZoneAlarm Pro examines outgoing packets before encryption, and incoming packets after decryption. This prevents malicious traffic from making its way into the VPN tunnel from your computer; and prevents any malicious traffic that might arrive on your computer via the VPN tunnel from doing any damage.

In order to configure ZoneAlarm Pro to protect VPN traffic, do the following:

1. Add the elements listed below to your Trusted Zone

- Your VPN server or VPN concentrator
- All of the LAN/WAN subnets that interact with the internal network that you want access to.
- Any servers that you will need to make use of through the VPN but are not on your internal network, such as DNS, POP, or SMTP servers.
- RADIUS or TACACS servers (if applicable).

Tip Contact your network administrator if you do not know the addresses or host names of the network elements listed.

2. If you receive a firewall alert caused by a blocked attempt to access your loopback address (127.0.0.1), add the loopback address to the Trusted Zone, and make sure there is no proxy software running on your computer. See *Zones tab*, page 82.
3. In the Security tab (Advanced Settings dialog box), select Allow VPN protocols at high security. See *Security tab*, page 88.
4. If your VPN uses protocols other than GRE, ESP and AH, also select Allow uncommon protocols at high security.

ICS (Internet Connection Sharing)

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, you can protect all of the computers that share the connection from inbound threats by installing ZoneAlarm Pro on the "gateway" machine only. However, to receive outbound (Program Control) protection, or to see alerts on the client machines, you must have ZoneAlarm Pro installed on the client machines as well.

Tip Before you configure ZoneAlarm Pro, use your ICS software to set up the gateway and client relationships. If you use hardware such as a server or router, rather than a host PC, to perform Internet connection sharing, do not follow the steps below.

On the ICS gateway machine:

1. Go to Overview tab of the Firewall panel.
2. Click **Advanced**.
3. Under Internet Connection Sharing, select **This computer is an ICS gateway**.
4. In the combination box, select or type the IP address of the gateway machine.
5. Select **Suppress alerts locally if forwarded to clients** if you do not want to see alerts on the gateway that are also displayed on the client. Note that if you do not install ZoneAlarm Pro on the client machines, all alerts will be displayed on the gateway.
6. For best security, make sure the security level for the Internet Zone is set to high. Make sure outgoing DNS and DHCP are allowed for the Internet Zone at high security.

On the ICS client machines:

1. Go to Overview tab of the Firewall panel.
2. Click **Advanced**.
3. Under Internet Connection Sharing, select **This computer is a client of an ICS gateway running ZA Pro**.
4. In the combination box, select or type the IP address of the gateway machine.
5. Select **Forward alerts from gateway to this computer** if you want alerts occurring on the gateway machine to be displayed on this client.

Proxy server

To enable your computer to connect to the Internet through a proxy server, add the proxy to your Trusted Zone. See Zones tab, page 82.

ISP heartbeat

Most ISPs periodically send "heartbeat" messages to their connected dial-up customers to make sure they are still there. If it appears a customer is not there, the ISP might disconnect her so that her IP address can be given to someone else.

By default, ZoneAlarm Pro blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet.

If this happens you can solve the problem in any of the three ways described below.

Identify the server sending the message and add it to your Trusted Zone.

This is the preferred solution, because it will work whether your ISP uses NetBIOS or ICMP to check your connection, and it allows you to maintain high security for the Internet Zone. To identify the server your ISP uses to check your connection, follow these steps:

1. Wait until your ISP disconnects you.
2. Go to the Alert Log tab (Alerts & Logs panel).
3. In the alerts list, find the alert that corresponds to the time you were disconnected.

If you're not able to identify the server this way, contact your ISP. They should be able to tell you what servers your need to allow.

After you have identified the server, add it to the Trusted Zone.

Allow ping messages through the Internet Zone.

If your ISP uses ICMP echo (or ping) messages for connectivity checks, use the Internet Zone tab (Custom Securities dialog box) to configure ZoneAlarm Pro to allow ping messages from the Internet Zone. To do this:

1. Go to the Main tab in the Firewall Panel.
2. In the Internet Zone section, click **Custom**
3. Select check box labeled **Allow incoming ping (ICMP echo)**.
4. Click **OK**.

Set the security level for the Internet Zone to medium.

The quickest but least secure solution is to reduce the security level for the Internet Zone to medium.

Customizing your security

If you're not the "set it and forget it" type, ZoneAlarm Pro enables you to manage the details of your Internet security.

Firewall protection

Block or unblock ports

ZoneAlarm Pro's preconfigured security levels (Low, Medium, and High) specify the ports that are open or closed to each Zone. Customize security levels by blocking or unblocking specific ports in the Internet Zone tab and the Trusted Zone tab.

Use the Security tab to customize general firewall options. See *Internet Zone tab*, page 84, *Trusted Zone tab*, page 86, and *Security tab*, page 88.

Program control

Allow or block new programs

ZoneAlarm Pro asks your permission each time a new program wants access or server rights. To avoid seeing these alerts, you can automatically allow or block new programs using the Access Permissions tab. See *Access Permissions tab*, page 99.

Specify the ports a program can use

By default, programs given access permission or server permission can use any port. Tighten program security by specifying the types of servers each program can access, and the ports it can and cannot use, in the Ports tab. See *Ports tab*, page 102.

Customize authentication for a program

For each program, you can specify whether ZoneAlarm Pro will authenticate the base executable only, or the executable and the components it loads. If a program is frequently updated, you can avoid repeated alerts by using file path authentication only. Choose these options in the Security tab of the Program Options dialog box. See *Security tab*, page 104.

Alerts and logs

Show or hide informational alerts for specific firewall events

By default, ZoneAlarm Pro displays informational alerts for firewall events only if they are likely to have resulted from hacker activity. You can customize alert display by enabling or suppressing alerts for specific events in the Alert Events tab. See *Alert Events tab*, page 110.

Enable or suppress logging for firewall events

You can also enable or suppress log entries for specific firewall events, also in the Alert Events tab.

Enable or suppress logging for program events

By default, ZoneAlarm Pro creates a log entry when any type of Program alert occurs. You can customize Program alert logging by suppressing log entries for specific Program alert types, such as New Program alerts, Repeat Program alerts, or Server Program alerts, in the Program Logs tab. See *Program Logs tab*, page 109.

Privacy protection

Block or allow cookie types

The default cookie control setting blocks only third-party cookies. You can also choose to block session and/or persistent cookies, set an expiration time limit for persistent cookies, and do other customization by using the Cookies tab. See *Cookies tab*, page 119.

Block or allow ad types

The default ad blocking setting blocks pop-up ads and slow-loading ads. You can choose to block all ads, change the time limit for banner and skyscraper ads to load, or choose what to display in place of blocked ads by using the Ad blocking tab. See *Ad Blocking tab*, page 121.

Block or allow mobile code types

By default, mobile code protection is turned off. You can block scripts, embedded objects, and/or MIME-type integrated object by turning mobile code protection on in the Main tab of the Privacy panel. Customize the types of code to block by using the Mobile Code tab. See *Mobile Code tab*, page 122.

E-mail protection

Quarantine or allow specific attachment types

MailSafe quarantines 37 types of e-mail attachments. You can turn off quarantining for any type of attachment, or add more types of attachments to the quarantine list, in the Attachments tab. See *Attachments tab*, page 124.

Reading the ZoneAlarm Pro log

Viewing the Log

To view the current log in the Log Viewer:

- In the Alerts & Logs panel, choose the Log Viewer tab.

To view the current log as a text file:

1. In the Main tab of the Alerts & Logs panel, click the **Advanced** button. The Advanced Alerts & Log Settings dialog box opens.
2. Choose the Log Control tab.
3. Under Log Archive Location, click the **View Log** button.

Note By default, alerts generated by ZoneAlarm Pro are logged in the file ZALog.txt. If you are using Windows95, Windows98 or Windows Me, the file is located in the following folder: (x):\Windows\Internet Logs. If you are using WindowsNT or Windows2000, the file is located in the following folder: (x):\Winnt\Internet Logs.

Log fields

Log entries contain the fields described in the table below.

Field	Description	Example
Type	The type of event recorded (see "Event types" below).	FWIN
Date	The date of the alert, in format yyyy/mm/dd	2001/12/31(December 31, 2001)
Time	The local time of the alert. This field also displays the hours difference between local and Greenwich Mean Time (GMT).	17:48:00 -8:00GMT (5:48 PM, eight hours earlier than Greenwich Mean Time. GMT would be 01:48.)
Source	The IP address of the computer that sent the blocked packet, and the port used; OR the program on your computer that requested access permission	192.168.1.1:7138 (FW events) Microsoft Outlook (PE events)
Destination	The IP address and port of the computer the blocked packet was addressed to.	192.168.1.101:0
Transport	The protocol /packet type	UDP

type) involved.

Event types

The first field in a log entry indicates the type of event recorded.

Event type code	Meaning
FWIN	The firewall blocked an inbound packet of data coming to your computer. Some, but not all, of these packets are connection attempts.
FWOUT	The firewall blocked an outbound packet of data from leaving your computer.
FWROUTE	The firewall blocked a packet that was not addressed to or from your computer, but was routed through it.
FWLOOP	The firewall blocked a packet addressed to the loopback adapter (127.0.0.1)
PE	An application on your computer requested access permission.
ACCESS	Program Control prevented an application on your computer from accessing remote resources.
LOCK	The firewall blocked a packet because the Internet Lock was engaged.
MS	MailSafe quarantined an e-mail attachment

ICMP message types

When ZoneAlarm Pro blocks an ICMP packet, the log displays a number indicating what type of ICMP message it was.

- 0 - Echo Reply
- 3 - Destination Unreachable
- 4 - Source Quench
- 5 - Redirect
- 8 - Echo Request

- 9 - Router Advertisement
- 10 - Router Solicitation
- 11 - Time Exceeded
- 12 - Parameter Problem
- 13 - Timestamp Request
- 14 - Timestamp Reply
- 15 - Information Request
- 16 - Information Reply
- 17 - Address Mask Request
- 18 - Address Mask Reply

TCP flags

The TCP Flags are:

- S (SYN)
- F (FIN) R (RESET)
- P (PUSH)
- A (ACK)
- U (URGENT)
- 4 (low-order unused bit)
- 8 (high-order unused bit)

Sample log entries

Sample 1: FWIN

FWIN,2000/03/07,14:44:58,-8:00 GMT, Src=192.168.168.116:0, Dest=192.168.168.113:0, Incoming, ICMP

FWIN indicates that the firewall blocked an incoming request to connect to your computer. The entry also includes the following information:

- Date and Time
- Source IP Address and port number
- Destination IP Address and port number
- Transport-Indicates that the transport was either TCP, UDP, ICMP, or IGMP

Sample 2: FWOUT

FWOUT,2000/03/07,14:47:02,-8:00 GMT,QuickTime Player Application tried to access the Internet. Remote host: 192.168.1.10

ZoneAlarm Pro blocked an outbound request. FWOUT indicates that the firewall blocked an outbound request from your computer. The entry also includes the following information:

- Date and Time
- Source IP Address and port number
- Destination IP Address and port number
- Transport-Indicates that the transport was either TCP, UDP, ICMP, or IGMP

Sample 3: PE

PE,2000/03/22,17:17:11 -8:00 GMT,Netscape Navigator application file,192.168.1.10

The PE entry informs you that an application on your computer attempted to access the Internet. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address and Port number that the application was trying to connect to.

Sample 4: LOCK

LOCK,2000/09/07,16:43:30 -7:00 GMT,Yahoo! Messenger,207.181.192.252,N/A

The LOCK entry informs you that an application on your computer attempted to access the Internet while the Internet Lock was engaged. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address that the application was trying to connect to.

Sample 5: ACCESS

ACCESS,2000/09/07,16:45:57 -5:00 GMT,Microsoft Internet Explorer was not allowed to connect to the Internet (64.55.37.186).,N/A,N/A

The ACCESS entry informs you that Program Control prevented an application on your computer from accessing remote resources. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address that the application was trying to connect to.

Sample 6: MS

MS,2000/09/08,09:45:56 -5:00 GMT,Microsoft Windows(TM) Messaging Subsystem Spooler,Renamed e-mail attachment of type .HLP to .zla,N/A

The MS entry informs you that an e-mail containing an attachment of a file type that you have asked MailSafe to quarantine was received by your e-mail client. The entry also includes the following information:

- Date and Time
- The system that handles e-mail delivery on your system, like Microsoft Windows(TM) Messaging Subsystem Spooler
- The name of the file, including file type, that was quarantined.

5 Interface Guide

The ZoneAlarm Pro dashboard



Inbound/Outbound traffic indicator



The traffic indicator shows you when traffic leaves (red) or enters (green) your computer. This does not imply illegal traffic or any security problem.

Note Some applications access network resources in the background, so you may see network traffic occurring even when you aren't actively accessing the Internet.

Stop button (Emergency Panic Lock)



Click the **Stop** button to immediately stop all inbound and outbound traffic. Click again to disengage.

Tip Use the Stop button only in emergencies. For more information, see the related topic *Using the Internet Lock and Stop button*

Networks



The networks indicator shows you when you have wired or wireless networks in either the Trusted Zone or Internet Zone. In the example at left, there is one wired network in the Trusted Zone.

Click the network symbol to go immediately to the Zones tab, where the settings for the network are stored.

Internet Lock

Click the lock icon to close the Internet lock. Click again to disengage.



This view indicates the lock is **open**.



This view indicates the lock is **closed**.

Note Use the Internet Lock to protect your computer if you leave it connected to the Internet but inactive for long periods. For more information , see the related topic *Using the Internet Lock and Stop button*

Active programs



The active programs area displays the icons of programs that are currently open and that have accessed the Internet in your current session.

The icon blinks when the program is sending or receiving data.

A hand symbol under the icon indicates that the program is [active as server](#) and is listening for connection requests.

To see information about a program displayed here, hover your mouse pointer over the icon.

All systems active

This area can display two messages.

- The message **All Systems Active** indicates that ZoneAlarm Pro is functioning normally.
- The message **Error. Please Reboot** indicates that you are not protected by ZoneAlarm Pro because the underlying security process is not running. Restart your computer to allow ZoneAlarm Pro to reset.

Overview Panel

Status tab



Use the Status tab to:

- See at a glance if your computer is secure
- See a summary of ZoneAlarm Pro's activity
- See if your version of ZoneAlarm Pro is up to date
- Access the ZoneAlarm Pro tutorial

1 – Blocked Intrusions

Blocked Intrusions shows you how many times the ZoneAlarm Pro firewall and MailSafe have acted to protect you, and how many of the alerts were high-rated.

2 - Protection

The protection area tells you at a glance whether your firewall, program, and e-mail security settings are safe. It also summarizes security activity of each type.

Tip To reset the alert counts in this area, click **Reset to Default** at the bottom of the panel.

Inbound Protection

Use this area to see:

- If your firewall is configured safely. ZoneAlarm Pro will warn you if firewall security is set too low.
- How many Firewall alerts, MailSafe alerts, and Internet Lock alerts have occurred since the last reset.

Outbound Protection

Use this area to see:

- If program control is configured safely. ZoneAlarm Pro will warn you if program security is turned off.
- How many Program alerts have occurred since the last reset.

E-mail Protection

Use this area to see MailSafe is on. The text message shows you how many attachments have been quarantined since the last reset.

Tip Click the underlined text of any warning (for example, "Program control is off") to go immediately to the panel where you can change that setting.

3 - Reset to Default

Clicking the **Reset to Default** link returns the event counters in the Inbound Protection, Outbound Protection, and E-mail protection areas to 0. These counters are also reset if you uninstall and reinstall ZoneAlarm Pro.

4 - Update and tutorial information

Click **ZoneAlarm Pro Tutorial** to learn the basics of how ZoneAlarm Pro works.

Update box

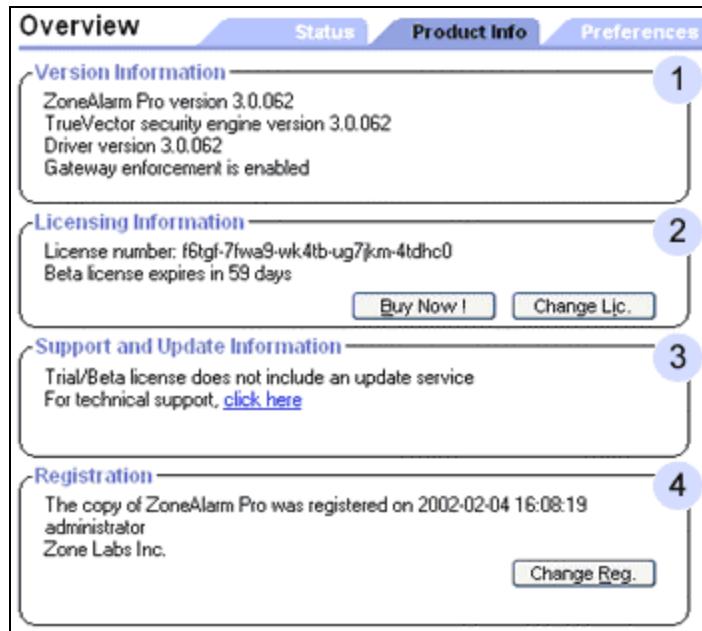
The update box helps you make sure you're running the latest version of ZoneAlarm Pro, and gives you quick access to product updates when they arrive.

Message	Meaning
"Check for update"	Click the link to see if there are any important updates to ZoneAlarm Pro available for download.
"An update is available."	Your automatic update subscription indicates an update to ZoneAlarm Pro is available. Click the link to go to the Zone Labs Web site to obtain the update.
"Update subscription expired"	Your automatic update subscription has expired. Click the link to renew it.

Click to
renew."

Note When you purchase ZoneAlarm Pro, you receive an automatic update subscription valid for one year.

Product Info tab



The Product Info tab gives you quick access to information about your version of ZoneAlarm Pro.

Use this tab to:

- See what version of ZoneAlarm Pro you have.
- Change your License key.
- Access the Technical Support area of the Zone Labs Web site.
- Change your registration.

1 - *Version Information*

This area shows what version of ZoneAlarm Pro, and what version of the TrueVector security engine, are running on your computer.

Tip To see if there is a new version available, go to the Status tab in the Overview panel, and check the update information on the right side of the screen.

If you have a gateway license, this area also indicates whether [gateway enforcement](#) is turned on or off. "Gateway enforcement is active" indicates that ZoneAlarm Pro has established communication with the gateway.

2 - Licensing Information

This area displays your ZoneAlarm Pro license number. If you are using a trial version of ZoneAlarm Pro, it tells you how many days are remaining in your trial period.

Click **Buy Now!** to upgrade from a trial version of ZoneAlarm Pro.

Click **Change Lic.** to change the license key under which your version of ZoneAlarm Pro is operating.

3 – Support and update information

This area shows the status of your [product update service](#). If your service has expired or is about to expire, click **Renew** to continue to get automatic updates to ZoneAlarm Pro.

Follow the technical support link to access FAQ, troubleshooting, and other technical information on the Zone Labs Web site.

Tip Before contacting Zone Labs technical support, try the troubleshooting steps provided in this help system. Start at the help [welcome page](#).

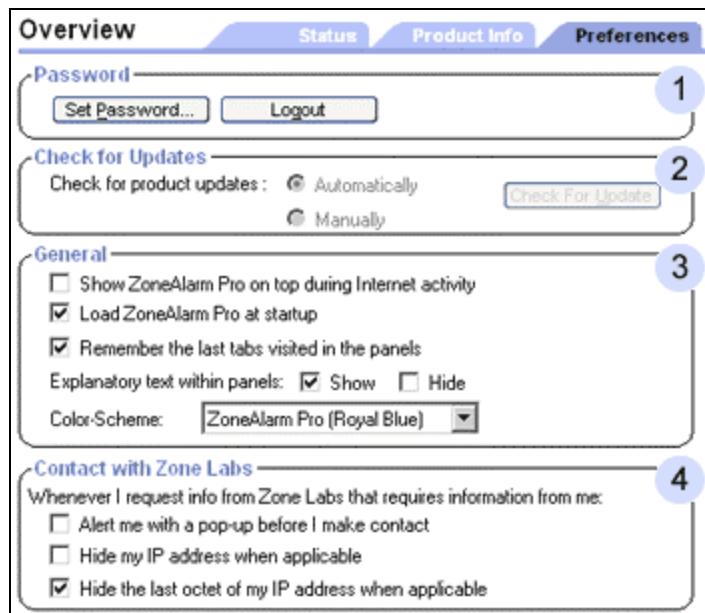
4 - Registration

This area shows whether you have registered your copy of ZoneAlarm Pro. If your registration is "pending", you have submitted registration information, but ZoneAlarm Pro has not yet received confirmation of registration from Zone Labs.

Click **Change Reg.** to edit your registration information (name, company, or e-mail).

Click **Register** to register online. Registration only takes a few seconds.

Preferences tab



Use the Preferences tab to:

- Set or change your ZoneAlarm Pro password.
- Log in or log out.
- Configure ZoneAlarm Pro to automatically notify you of product updates.
- Set general options for the display of the ZoneAlarm Pro Control Center.
- Configure privacy settings for communications with Zone Labs.

1 – Password

By setting a password, you prevent anyone but you from shutting down ZoneAlarm Pro, or changing your security settings.

Once you have set a password, you must log in before you can change settings, shut down the TrueVector security engine or uninstall ZoneAlarm Pro.

Valid passwords are between 6 and 31 characters long. Valid characters include A-Z, a-z, 0-9, and characters !,@,#,\$,%,^,&,*.

Note Setting a password will not prevent other people from accessing the Internet from your computer.

2 – Check for Updates

Select **Automatically** to have ZoneAlarm Pro automatically notify you of available updates.

If you would rather check for upgrades yourself by looking in the Status tab of the Overview panel, select **Manually**.

Tip These controls are enabled only if you have purchased ZoneAlarm Pro and if you have a current subscription to the ZoneAlarm Pro product update service.

3 - General

Select **Show ZoneAlarm Pro on top during Internet activity** to have the ZoneAlarm Pro window come to the top of all other open windows whenever Internet activity occurs.

Select **Load ZoneAlarmPro at startup** to have ZoneAlarm Pro start automatically whenever you turn your computer on.

Select **Remember the last tabs visited in the panels** to have ZoneAlarm Pro start on the tab you had open the last time you closed the Control Center.

Select **Show or Hide** to show or hide the explanatory text that appears to the left of each ZoneAlarm Pro tab. If you select **Hide**, you can still display the text for any panel by clicking the **Show Text** link at the bottom.

4 – Contact with Zone Labs

These controls enable you to protect your privacy when ZoneAlarm Pro communicates with Zone Labs.

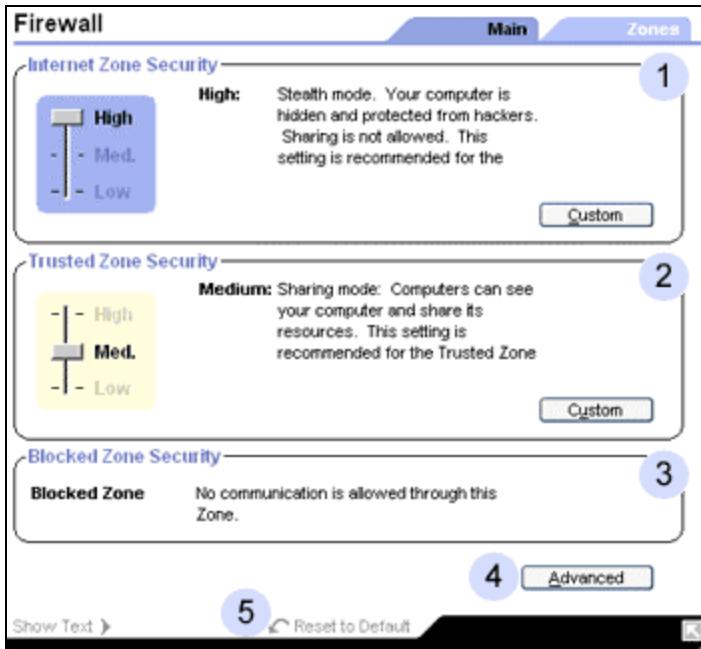
Select **Alert me with a pop-up before I make contact** to have ZoneAlarm Pro warn you before it contacts Zone Labs to deliver registration information, get product updates, or find more information about an alert.

Select **Hide my IP address when applicable** to not include your IP address when you submit an alert to Zone Labs AlertAdvisor. This prevents Zone Labs, as well as anyone else who might intercept the message, from identifying your computer.

Select **Hide the last octet of my IP address** to not include the last three digits (for example, 123.456.789.XXX) of your IP address when you access AlertAdvisor.

Firewall panel

Main tab



Use this tab to choose the basic level of security ZoneAlarm Pro will apply to traffic from computers you know and trust (the Trusted Zone) and computers you don't know (the Internet Zone).

To learn about Zones, see *What is a Zone?*, page 12.

1 - Internet Zone Security

Use the slider to set the security level for the Internet Zone. The recommended security level for the Internet Zone is **High**.

Click the **Custom** button to open the Internet Zone tab, where you can block or unblock specific ports. See also *Internet Zone tab*, page 84.

About Internet Zone security levels

- **High** security puts your computer in stealth mode. Windows (NetBIOS) services and file and printer shares are blocked. Ports are opened only when a program to which you have given permission needs them.
- **Medium** security takes your computer out of stealth mode, making it visible to other computers on the Internet. Windows services are still blocked. Program permissions are still enforced.
- **Low** security enables Windows services. Your computer is visible to others, and file sharing is allowed. Program control is still enforced

4 - Trusted Zone Security

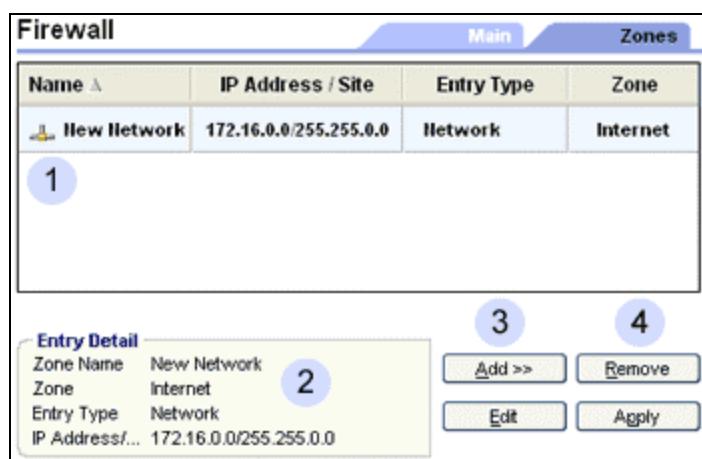
Use the slider to set the security level for the Trusted Zone.

Click the **Custom** button to open the Trusted Zone tab, where you can block or unblock specific ports. See also *Trusted Zone tab*, page 86.

About Trusted Zone security levels

- **High security** puts your computer in stealth mode. Windows (NetBIOS) services and file and printer shares are blocked. Ports are opened only when a program you have given access permission or server permission needs them. Programs must have your permission in order to access the Internet or local network.
- **Medium security** takes your computer out of stealth mode, making it visible to other computers on the Internet. File and printer sharing, as well as Windows services (NetBIOS), are enabled. Programs must still have permission to access the Internet or local network.
- **Low security** enables Windows services. Your computer is visible to others, and file sharing is allowed. A program control is still enforced.

Zones tab



The Zones tab contains the traffic sources (computers, networks, or sites) you have added to the Trusted Zone or Blocked Zone. It also contains any networks that ZoneAlarm Pro has detected. Use this tab to:

- Move a detected network to a different Zone.
- Move a computer, host, or site to a different Zone.
- Manually add a computer, host, site, or subnet to the Trusted Zone or Blocked Zone.

Tip If you are using a single, non-networked PC, you don't need to use this tab. The traffic source list displays only your ISP's network, which should be in the Internet Zone.

1 – Traffic source list

The list displays the traffic sources and the Zones they belong to. You can sort the list by any field by clicking the column header. The arrow next to the header name indicates the sort order. Click the same header again to reverse the sort order.

Traffic source list fields

Field	Information
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source
Entry Type	The type of traffic source this is: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked.

Changing the Zone of a traffic source

To change the Zone of a traffic source, left-click click in the Zones column for the source, then select from the shortcut menu.

Adding, removing, or editing a traffic source

To add, remove, or edit a traffic source, right-click in the Zones column for the source, then select from the shortcut menu.

Tip You must click the **Apply** button to save your changes.

2 – Entry detail window

The entry detail window displays information about the traffic source currently selected in the traffic source list. The fields are the same as those in the traffic source list.

3 – Add/Edit buttons

To add a traffic source to the list, click the **Add** button and select the type of traffic source you want to add from the shortcut menu. The Add dialog box opens.

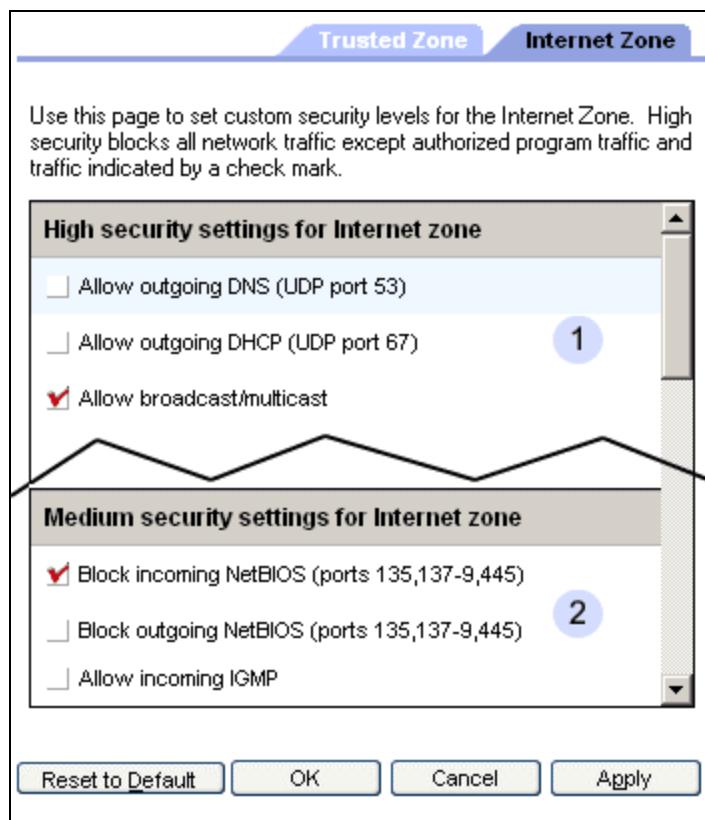
To change the Zone or any other information about a traffic source already in the list, select the traffic source, then click the **Edit** button. The Edit dialog box opens.

4 – Remove/Apply buttons

To remove a traffic source from the list, select it, then click the **Remove** button.

To save any changes you have made in this tab, click the **Apply** button.

Internet Zone tab



Use this dialog box to customize high security and medium security settings for traffic to and from the Internet Zone.

1 – High security settings for the Internet Zone

These are the port and protocol restrictions applied to the Internet Zone when **High** security is selected in the Main tab of the Firewall panel.

Tip To view the settings for medium security, scroll down below the high security settings.

Default configuration

The default configuration for high security blocks all inbound and outbound traffic through ports not being used by programs you have given access or server permission except:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67) (on Windows (9x systems)
- Outgoing DNS (port 53) (If the machine is configured as an ICS gateway in the Security tab.)

Allowing Additional Ports

You can allow communication through additional ports at high security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying ports. To specify ports, follow these steps:

1. Scroll to the bottom of the high security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled Ports appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to allow in the Ports text box, separated by commas.
Example: 139, 200-300
4. Click **Apply** or **OK**.

2 – Medium security settings for the Internet Zone

These are the port and protocol restrictions applied to the Internet Zone when **Medium** security is selected in the Main tab of the Firewall panel.

Default configuration

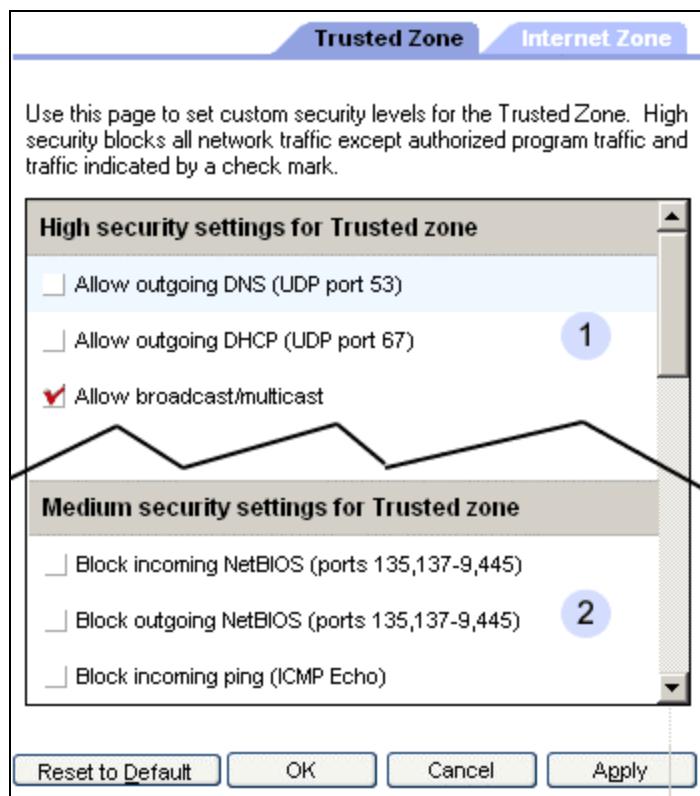
The default settings for medium security allow inbound and outbound traffic through all ports except of incoming NetBIOS traffic (ports 135, 137-139, 445). The NetBIOS protocol enables file and printer sharing on local networks. It is blocked at medium security for the Internet Zone because, if exposed to the Internet, it is vulnerable to common intrusion attempts.

Blocking Additional Ports

You can block additional ports at medium security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying ports. To specify ports, follow these steps:

1. Scroll to the bottom of the medium security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled Ports appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to block in the Ports text box, separated by commas.
Example: 139, 200-300
4. Click **Apply** or **OK**.

Trusted Zone tab



Use this dialog box to customize high security and medium security settings for traffic to and from the Trusted Zone.

1 – High security settings for the Trusted Zone.

These are the port and protocol restrictions applied to the Trusted Zone when **High** security is selected in the Main tab of the Firewall panel.

Tip To view the settings for **Medium** security, scroll down below the high security settings.

Default configuration

The default settings for high security block all inbound and outbound traffic through ports not being used by programs you have given access or server permission, with the following exceptions:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67) (On Windows 9x systems)
**
- Outgoing DNS (port 53) (If the machine is configured as an ICS gateway in the Security tab.)

These protocols are permitted because they are central to basic Internet addressing functions and do not represent a serious security risk.

Allowing Additional Ports

You can allow communication through additional ports at high security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying a port number. To specify a port number, follow these steps:

1. Scroll to the bottom of the high security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled Ports appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to allow in the Ports text box, separated by commas.
Example: 139, 200-300
4. Click **Apply** or **OK**.

2 – Medium security settings for the Trusted Zone

These are the port and protocol restrictions applied to the Trusted Zone when Medium security is selected in the Main tab of the Firewall panel.

Default configuration

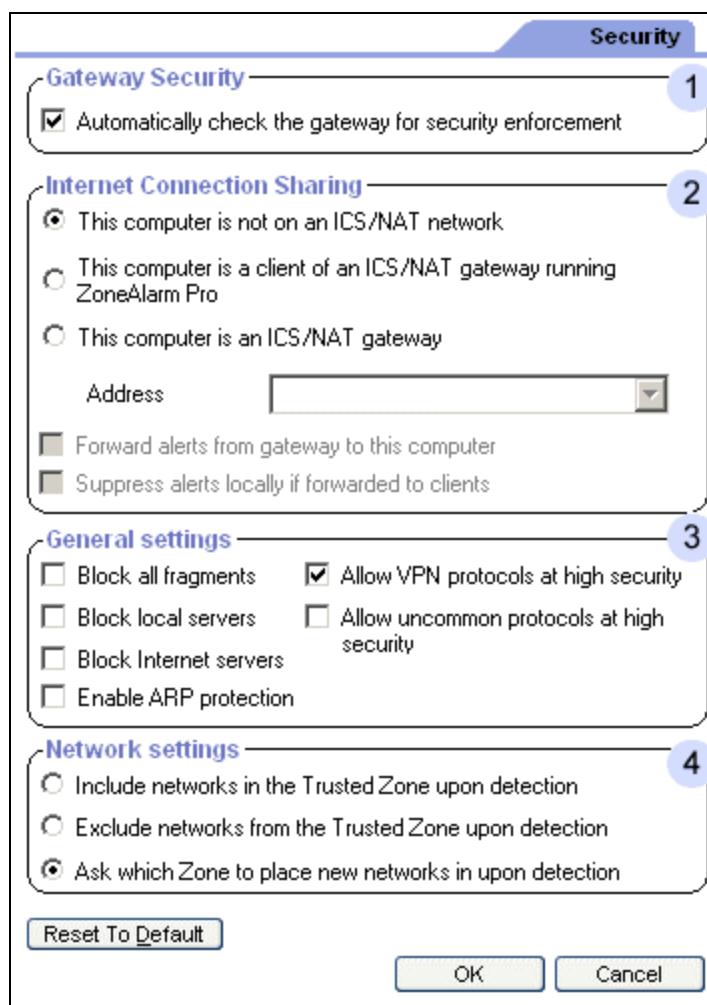
The default settings for medium security ALLOW all inbound and outbound traffic through all ports, INCLUDING incoming NetBIOS traffic (ports 135, 137-139, 445). The NetBIOS protocol enables file and printer sharing on local networks.

Blocking Additional Ports

You can block additional ports at medium security either by selecting one of the preconfigured protocols (ICMP, IGMP, and so forth), or by specifying a port number. To specify a port number, follow these steps:

1. Scroll to the bottom of the medium security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled Ports appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to block in the Ports text box, separated by commas.
Example: 139, 200-300
4. Click **Apply** or **OK**.

Security tab



Use the Security tab in the Advanced Settings dialog box to establish global network and security settings.

1 – *Gateway security*

Some companies require their employees to use ZoneAlarm Pro when connecting to the Internet through their corporate gateway. When this control is selected, ZoneAlarm Pro checks for any compatible gateways and confirms that it is installed, so that gateways requiring ZoneAlarm Pro will grant Internet access.

You can leave this control selected even if you are not connecting through a gateway; it will not affect your Internet functions.

If you are on a network that uses gateway enforcement, and this control is not selected, you will not be able to access the network.

2 – Internet Connection Sharing

If you are using Internet Connection Sharing, use these controls to configure ZoneAlarm Pro to recognize the ICS gateway and clients.

Use the radio buttons to indicate whether your computer is an ICS client, or an ICS gateway. ZoneAlarm Pro automatically detects the IP address of the ICS gateway and displays it in the **Address** box. This box is labeled **Local Address** if you are the gateway, and **Gateway Address** if you are the client.

Note For ICS clients running ZoneAlarm Pro to work properly, the ICS gateway must run ZoneAlarm Pro as well.

Alert forwarding

You can determine whether the alerts that occur on an ICS network will be displayed and logged on the gateway, on the client, or on both.

If you are working on a client machine, select **Forward alerts from gateway to this computer** to have alerts that occur on the gateway computer appear and be logged on the client computer.

If you are working on a gateway, select **Suppress alerts locally if forwarded to clients** if you do not want alerts forwarded from the gateway to clients to also be displayed on the gateway.

See also *Internet Connection Sharing* , page 63.

3 – General Settings

These controls apply global rules regarding certain protocols, packet types and other forms of traffic (such as server traffic) to both the Trusted Zone and the Internet Zone.

Control	Function when selected
Block all fragments	Blocks all incomplete (fragmented) IP data packets.
Block local servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.
Block Internet servers	Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.
Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target machine. Also blocks all incoming ARP replies except those in response to

	outgoing ARP requests.
Allow VPN Protocols at high security	Allows the use of VPN protocols (ESP, AH, GRE) even when high security is applied. When this control is not selected, these protocols are allowed only at medium security.
Allow uncommon protocols at high security	Allows the use of uncommon protocols. When this control is not selected, these protocols are allowed only at medium security.

4 – Network Settings

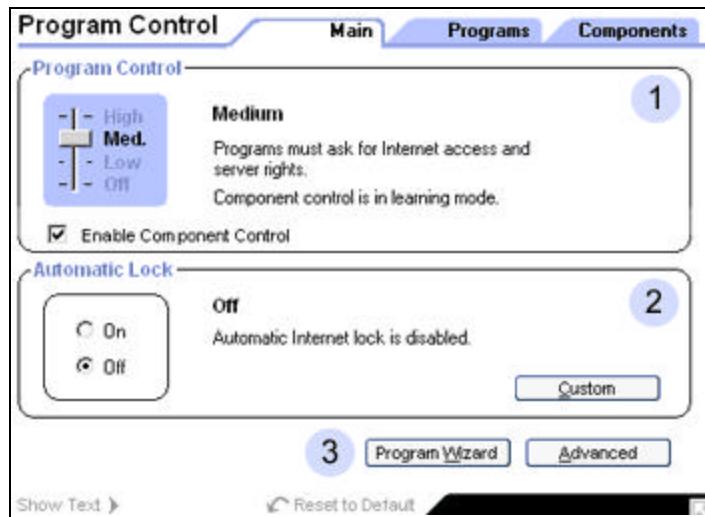
Automatic network detection helps you configure your Trusted Zone easily, so that traditional local network activities such as file and printer sharing aren't interrupted.

You can have ZoneAlarm Pro silently include or exclude every detected network in the Trusted Zone; or ask you in each case whether the newly detected network should be added.

Note ZoneAlarm Pro detects only networks that you are physically connected to. Routed or virtual network connects are not detected.

Program Control panel

Main tab



Use this panel to choose a program control level, and to turn the Internet Lock on or off.

1 – Program Control

Use the slider to choose a global setting for program control. Use the check box to turn component control on or off.

Tip Zone Labs recommends the default **Medium** setting for the first few days of normal use. This enables ZoneAlarm Pro to learn and secure your program components. ZoneAlarm Pro will remind you to raise program control to **High** after a few days.

High setting

When a program accesses the Internet, ZoneAlarm Pro authenticates it as well as the components it is using. If the program's MD5 signature, file name, or location has changed, a Changed Program alert is displayed. If the program is using a new component, or a component whose signature has changed, a Program Component alert is displayed.

Program permissions are enforced. The following program alerts can occur under this setting:

- New/Repeat/Server Program
- Changed Program
- Program Component

Medium setting

ZoneAlarm Pro authenticates the program, and "learns" the components the program is using, adding them to the components list and recording their MD5 signatures. Later, if program control is set to **High**, the recorded component signatures are used for authentication.

Program permissions are enforced. The following program alerts can occur under this setting:

- New/Repeat/Server Program
- Changed Program

Low setting

ZoneAlarm Pro "learns" your programs and their components by recording their signatures, but does not authenticate them. Later, if authentication is set to High, the recorded signatures are used for authentication. New Program and Repeat Program alerts are still displayed, but Changed Program alerts are not.

Program permissions are enforced. The following program alerts that can occur under this setting:

- New/Repeat/Server Program

Off

No program authentication is performed. **No** program permissions are enforced. All programs are allowed access/server rights. **No** program alerts can occur.

2 – Automatic Lock

The Automatic Internet Lock protects your computer if you leave it connected to the Internet for long periods even when you're not using network resources.

If you turn the Automatic Lock **on**, the Internet Lock will engage when your screen saver engages OR after a specific number of minutes of network inactivity, depending on settings in the Auto Lock tab.

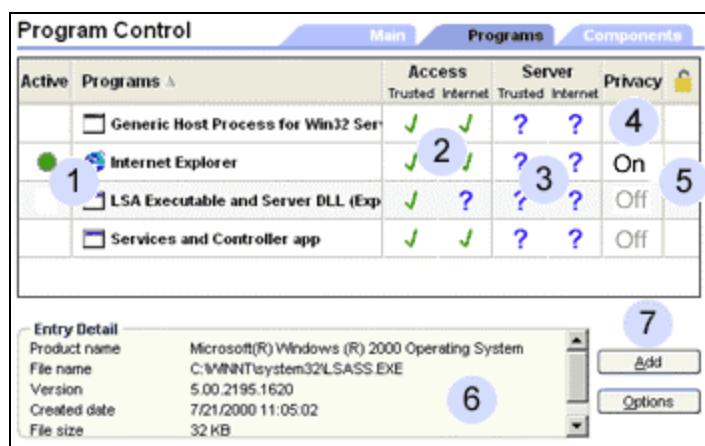
For more information about the Internet Lock, see *Using the Internet Lock and Stop button*, page 54.

3 – Program Wizard/ Advanced

Click the **Program Wizard** button to have the ZoneAlarm Pro program wizard help you set up your programs for Internet access.

Click **Advanced** to open the Advanced Program Settings dialog box, where you can use the Access Permissions tab and the Alerts & Functionality tab to customize program control options.

Programs tab



Use this tab to:

1. Grant or deny access permission and server permission to your programs
2. Add programs to the list and establish their permissions
3. Review your settings

Program permission symbols

- ✓ A green check means the program is allowed access/server rights.
- ✗ A red X means the program is denied access/server rights.
- ? A blue question mark means ZoneAlarm Pro will display a Program alert when the program asks for access/server rights.

Tip You can sort the programs in the list by any field. Click on the field header to sort. The arrow icon indicates the sort order.

1 – Program name and status

As you use your computer, ZoneAlarm Pro detects every program that requests network access and adds it to this list. It also records the answer you gave to the Program alert for that program. A green bullet in the Active column means the program listed is currently accessing network resources. The program column displays the program name and associated icon.

Tip For more information about a program, click the program name, then look in the Entry Details box at the bottom of the screen.

2 & 3 – Access permission/Server permission

Use these fields to establish access permission and server permission for a program.

Left-click menu

To change a permission setting, click the symbol, then select from the shortcut menu.

Right-click menu

Right-click anywhere in the program's row to select from a variety of other options. See the table below for a description of each option.

Option	Explanation
Changes Frequently	If this option is selected, ZoneAlarm Pro will use only file path information only to authenticate the program. The MD5 signature will not be checked. Caution This is a low-security setting.
Options	Opens the Program Options dialog box, in which you

	can customize port permissions and security options for the program.
Properties	Opens your operating system's properties dialog box for the program.
Remove	Deletes the program from the list.
Add program	Opens an explorer window so you can browse to a program on your computer that you want to add to the list.

Note Built-in rules ensure a consistent security policy for each program. Programs with access to the Internet Zone also have access to the Trusted Zone, and programs with server permission in a Zone also have access permission for that Zone. This is why (for example) selecting Allow under Trusted Zone/Server automatically sets all of the program's other permissions to Allow.

4 - Privacy

On indicates that privacy protection is enabled for the program. **Off** indicates that privacy protection is disabled.

To enable privacy protection for specific program, click in this column, then choose **Privacy On** from the shortcut menu.

To disable privacy protection for a program, click in this column, then choose **Privacy Off** from the shortcut menu.

5 – Pass-lock

A key in this field indicates that the program has pass-lock privilege.

To give pass lock privilege to a program, click the lock column, then choose **Pass-Lock** from the shortcut menu.

To revoke pass-lock privilege, click the lock icon, then choose **Normal** from the shortcut menu.

Tip If you grant pass-lock permission to a program, and that program uses other applications to perform its functions (for example, services.exe), be sure to give those other programs pass-lock permission as well

6 – Entry detail box

The entry detail box displays information about the program currently selected in the programs list.

Field	Information
Product name	The common name of the program, for example, Internet Explorer.
File name	The fully-qualified name of the executable file, for example, C:\Program Files\Internet Explorer\IEXPLORE.EXE
Version	The version number of the program.
Created date	The date the program was created by its manufacturer.
File size	The size of the executable file

7 - Add/Options buttons

Use these buttons to add a program to the programs list, or to access program options for the currently selected program.

Click **Add** to add a program to the programs list.

Click **Options** to access the Ports tab and Security tab in the Program Options dialog box.

For more information about the Program Options dialog, *Ports tab*, page 102 , and *Security tab*, page 104.

Components tab



About component security

ZoneAlarm Pro's component security feature prevents hackers from employing altered or falsified DLLs and other modules used by trusted programs in order to attack your computer. Without component security, malicious programmers could modify DLLs for your trusted programs, taking advantage of the Internet access permission given to the program's main executable in order to take control of your computer.

Using the components tab

Most users never need to use the components tab, because ZoneAlarm Pro automatically secures program components.

For advanced users, the Components tab enables detailed control of specific component files. Use this tab to determine whether:

Programs that are accessing network resources can load the listed component at will.

Programs that are accessing network resources must ask permission to load the listed component (ZoneAlarm Pro displays a Program Component alert)

Note **No** Program Component alerts are shown if Program Control is set to **Medium** or **Low** in the Main tab.

Component learning mode

Windows programs frequently load ten, twenty, or more components at a time in the course of normal operations.

Component "learning mode" enables ZoneAlarm Pro to quickly learn the MD5 signatures of many frequently-used components without interrupting your work with multiple alerts. The default **Medium** Program Control setting establishes component learning mode. We recommend that you use this setting for the first few days of normal Internet use after installing ZoneAlarm Pro.

After a few days of normal use, ZoneAlarm Pro will have learned the signatures of the majority of the components needed by your Internet-accessing programs, and will remind you to raise the Program Authentication level to **High**.

1 – Component access

The Component list automatically displays all components loaded by programs that have requested access permission or server permission.

Permission for a newly listed component is automatically set to **Allow** if:

You answered **Yes** to a Program Component alert or Component Loading alert

Program Control is set to Medium or lower (Component learning mode)

Permission for a new component is set to **Ask** if:

- You answered **No** to the Program Component alert.

Note: There is no **Block** option for components.

Changing component permissions

To change access permission for a component, click in the Access column, the select **Allow** or **Ask** from the shortcut menu.

Selecting multiple components

To select a range of components from the list:

5. Select a component by clicking it.
6. Hold down the SHIFT key while dragging the mouse upward or downward.

2 – Entry detail

The entry detail window displays information about the component currently selected in the list.

Field	Information
Component name	The common name of the component , for example, DHCP Client API DLL
File name	The fully-qualified name of the component, for example, C:\\WINNT\\system32\\dnsapi.dll
File type	The type of component, for example, Dynamic Link Library
Authentication	The method used to authenticate the component. Windows Protected System Files are automatically authenticated by ZoneAlarm Pro.
Version	The version number of the component.
Created date	The date the component was created.
File size	The size of the component file.
Last written	The last time this file was modified on your machine.
Last accessed	The last time this file was accessed by a program on your machine.

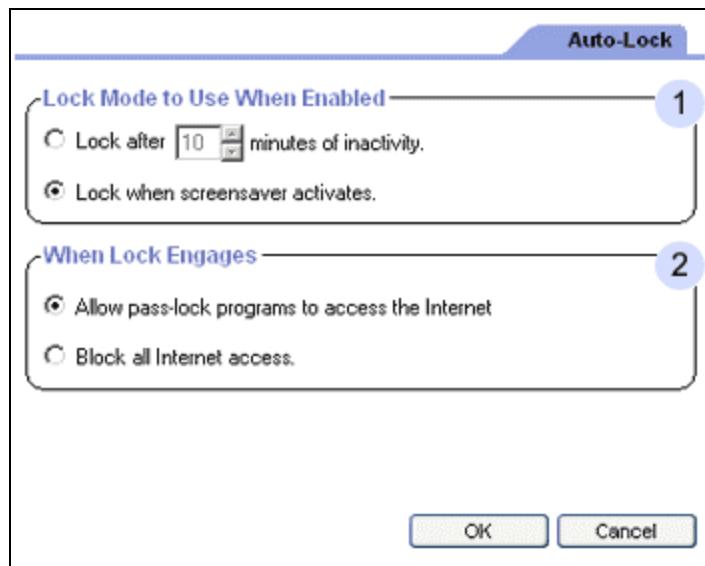
3 – Reset to default

Click this button to set the access permission for all components to Ask.

4 – More Info

Click the **More Info** button to learn more about program components from Zone Labs AlertAdvisor.

Auto-lock tab



Use these controls to determine:

- How the Automatic Internet Lock will engage
- Whether the lock will block all traffic, or allow [pass-lock](#) traffic.

Tip Settings in this tab go into effect only when the Automatic Internet Lock is turned on in the Program Control panel/Main tab.

For more information on the Internet Lock, see *Using the Internet Lock and Stop button*, page 54.

1 – Lock mode to use when enabled

You can set the automatic lock to engage either:

- After a period of Internet inactivity, or
- When your computer's screen saver activates.

Use the radio buttons to select a lock mode. If you choose the inactivity option, select the number of minutes of inactivity after which the lock will activate.

2 – When Lock engages

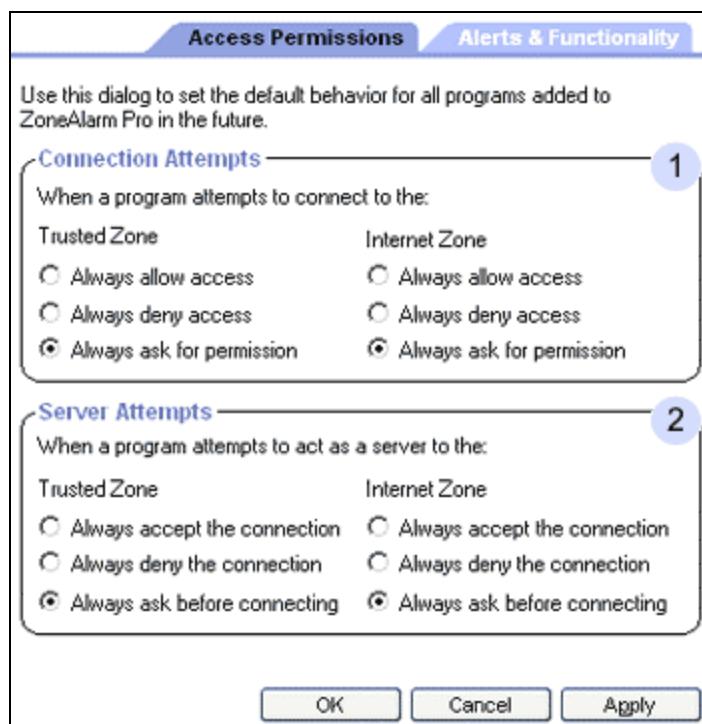
When the Internet Lock is engaged, it can either block all traffic, or continue to allow pass-lock traffic.

Allow the pass-lock programs to access the Internet is like the Internet Lock in the control bar. When the automatic lock engages, all traffic will be blocked, except traffic authorized by programs you have specifically given permission to bypass the lock.

Block all Internet access is like the **STOP** button in the control bar. When the automatic lock engages, all traffic to and from your computer will be blocked.

To find out how to give pass-lock permission to a program, *Programs tab*, page 92.

Access Permissions tab



By default, ZoneAlarm Pro displays a New Program alert when a program on your computer tries to access the Internet or local network resources for the first time. It displays a Server Program alert when a program tries to act as a server for the first time.

Use this tab to:

- Allow or deny access permission to all new programs
- Allow or deny server permission to all new programs.

You can apply different settings to each Zone.

Note Settings for individual programs can be established in the Programs tab. Settings in this panel apply ONLY to programs not yet listed in the Programs tab.

1 - Connection attempts

These settings determine what happens when a new program requests access permission for the Trusted Zone or Internet Zone.

Choose **Always deny...** to have ZoneAlarm Pro deny access silently

Choose **Always allow...** to have ZoneAlarm Pro allow access silently.

Choose **Always ask...** to have ZoneAlarm Pro show a New Program alert when a new program asks for access.

2 – Server attempts

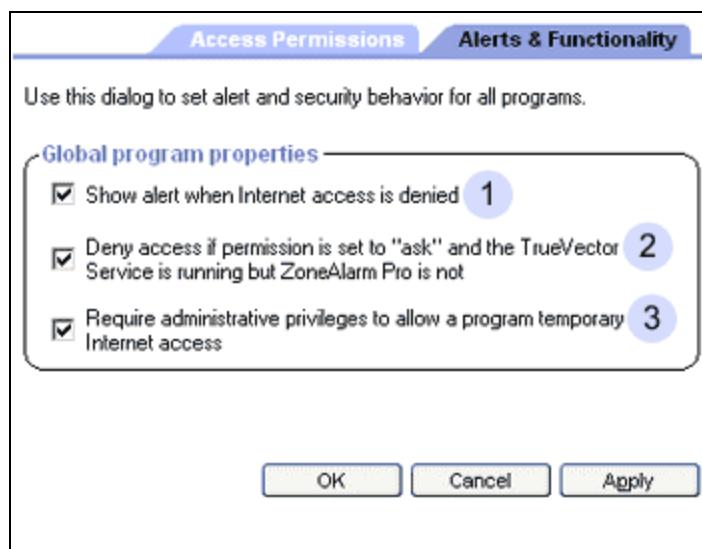
These settings determine what happens when a new program wants server permission for the Trusted Zone or Internet Zone.

Choose **Always deny...** to have ZoneAlarm Pro deny server rights silently

Choose **Always allow...** to have ZoneAlarm Pro allow server rights silently.

Choose **Always ask...** to have ZoneAlarm Pro show a Server Program alert when a new program asks for server rights.

Alerts & Functionality tab



The Alerts & Functionality tab provides access to advanced options for program control. These settings apply to all programs

1 – Show alert when access is denied

If ZoneAlarm Pro is set to deny Internet access to a particular program (for example, XProgram.exe in the example at left), but you want to be notified with an alert when it attempts to gain access anyway, select this option.

If you prefer to have ZoneAlarm Pro deny access silently, deselect this option

2 – Deny access if permission is set to “ask”

In rare cases, an independent process such as a Trojan horse could shut down the ZoneAlarm Pro user interface, but leave the TrueVector service running.

Without the interface, you would not see a Program alert when new program or a program set to "Ask" requests Internet access. This could cause the program to freeze.

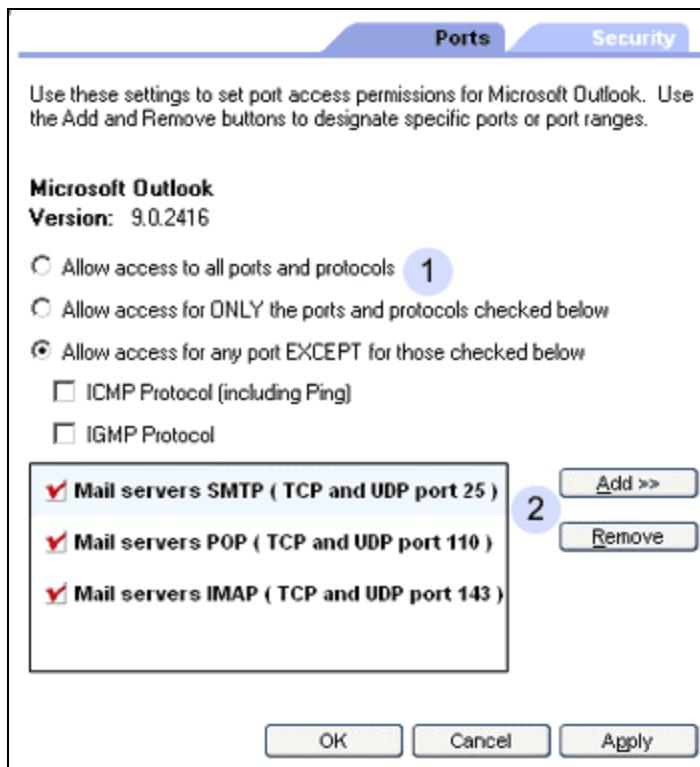
Select this option to have the TrueVector engine automatically deny access to any program set to "Ask". While the program won't be able to access network resources in this scenario, the automatic denial of access will leave it operational for other tasks.

3 – Require administrative privileges

If you protect your ZoneAlarm Pro settings with a password, you can't answer **Yes** to a program alert (thereby giving the program Internet access) unless you are logged in.

Deselect this option to allow someone who has not logged in with your ZoneAlarm Pro password to temporarily grant a program Internet access.

Ports tab



Use the Ports tab to specify the ports the selected program can use. For example, you can limit an e-mail client to SMTP, POP, and/or IMAP protocols. This provides an extra layer of security against program tampering.

Caution Use this tab to restrict a program's port access only you are very familiar with the needs of the program. Misconfiguring port permissions could cause your program to stop working properly.

1 – Port and protocol options

Choose from the following options:

- Allow access to all ports and protocols**

The program is able to access the Internet through all ports and use any necessary protocols. (When not in use by a permitted program the ports are protected by ZoneAlarm Pro's firewall).

- Allow access for ONLY the ports checked below**

Select this option to limit the program's access to a few ports and protocols.

- Allow access for any port EXCEPT for those checked below**

Select this option to exclude only a few ports from program access.

Tip If you choose either of the last two options, use the **Add** button to add ports to the list.

2 – Adding/removing custom ports

These controls are enabled only when **Allow access to all ports and protocols** is not selected. Use the **Add** and **Remove** buttons to modify the contents of the list.

Important! By adding to the list, you may be specifying ports the program can access (if you have selected **Allow access for ONLY the ports checked below**) or cannot access (if you have chosen **Allow access for any port EXCEPT for those checked below**). Be sure you have selected the option you intended!

To add ports to the list, click the **Add** button and select the server type from the shortcut menu. To add ports other than those associated with the server types listed, choose **Custom**. The Add dialog box will appear. For more information about the Add dialog box, click [here](#).

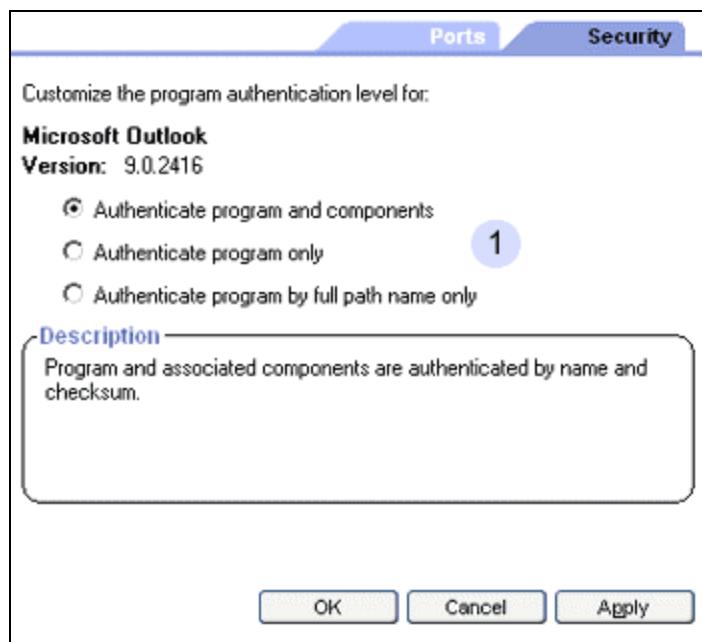
3- Add tab

Access this dialog box by choosing **Custom** from the Add shortcut menu.

To add a specific port or range of ports to the list:

1. Select the port type (TCP or UDP)
2. Type a description of the port (for display only)
3. Type the port number (if you're adding a single port) or the port range in the boxes provided, then click **OK**.

Security tab



Use this tab to choose the type of authentication to be used for this program.

When a program accesses network resources, ZoneAlarm Pro uses the selected authentication method to ensure that the program hasn't been tampered with. If the program has changed, ZoneAlarm Pro displays a Changed Program alert like the one at left.

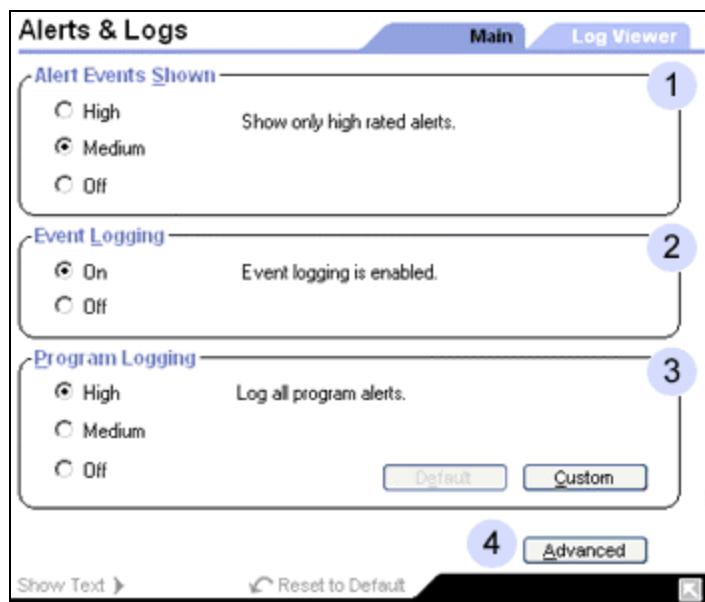
1 – Authentication options

Option	If selected
Authenticate programs and components	Whenever the program accesses the Internet or your local network, ZoneAlarm Pro uses the MD5 signature to verify that it is authentic and untampered with. If the program has loaded any components, ZoneAlarm Pro authenticates them as well.
Authenticate program only	ZoneAlarm Pro authenticates the program, but allows the program to load components without authenticating them.
Use program file path only	Instead of checking the MD5 signature, ZoneAlarm Pro will only check to see that the location of the program on your computer hasn't changed. This is a low-security option, but may be useful for programs that are frequently updated.

Tip Zone Labs suggests using the **Authenticate program only** option the first two times you use an application with ZoneAlarm Pro. This enables ZoneAlarm Pro to "fingerprint" the programs components silently. After using the application twice, select **Authenticate programs and components**, so that ZoneAlarm Pro will check all components against their fingerprints when a program accesses the Internet.

Alerts & Logs panel

Main tab



Use this tab to choose:

- What types of informational alerts ZoneAlarm Pro will display (all, high-rated only, or none).
- What types of informational alerts ZoneAlarm Pro will log.
 - What types of program alerts ZoneAlarm Pro will log.

Note Program alerts are always displayed, because they ask you to decide whether to grant program access or not.

For more information about informational alerts and program alerts, see *Responding to alerts*, page 38

1 – Alert events shown

This control determines what types of informational alerts ZoneAlarm Pro will display. The default Medium setting displays only high-rated alerts. The **High** setting displays all firewall alerts, both medium-rated and high-rated.

2 – Alert Events Logged

This control turns the logging of informational alerts informational alerts on and off.

3 – Program Logging

This control determines what types of program alerts are to be recorded in the ZoneAlarm Pro log.

The default **Medium** setting logs only high-rated alerts.

The **high** setting logs all program alerts.

Click the **Custom** button to customize program alert logging in the Program Logs tab.

If you have customized Program Logging settings, click the **Default** button to return to system defaults.

4 – Advanced

Click the **Advanced** button to open the Advanced Alerts and Log Settings dialog box. There you can:

- Specify alert display and logging by traffic type (Alert Events tab)
- Enable or disable the system tray icon alert (System Tray Alert)
- Configure your ZoneAlarm Pro log and set the archiving frequency (Log Control tab)

Log Viewer tab

The screenshot shows the 'Log Viewer' tab of the ZoneAlarm Pro interface. At the top, there is a text input field 'View only the last 999 alerts' with a '1' circled in blue. Below this is a table with five rows of alert data, each with a 'Medium' rating, a timestamp (2002/02/04 19:07:24-8:00 GMT), a 'Firewall' type, and 'UDP' protocol. A '2' is circled in blue next to the second row. At the bottom of the table is a 'More Info' button with a '4' circled in blue. To the left of the table is an 'Entry Detail' panel with fields: 'Description' (Packet sent from 172.16.100.170 (UDP Port 44...)), 'Direction' (Incoming), 'Type' (Firewall), and 'Source DNS' (RHPLAPTOP2.zonelabs.com). A '3' is circled in blue next to the 'Source DNS' field. At the bottom of the panel are 'Show Text' and 'Clear List' buttons, with a '5' circled in blue next to the 'Clear List' button.

The Log Viewer tab lists recent alerts. You can use each alert entry to:

- Submit the alert to Zone Labs AlertAdvisor for analysis.
- Add the source of the traffic that generated the alert to your Trusted Zone.

1 – View only the last *n* alerts

Select the number of alerts (starting with the most recent) to display in the alerts list.

2 – Alerts list

The alerts list shows Firewall alerts, Program alerts, and other alerts that have been recorded in the ZoneAlarm Pro log.

You can sort the list by any field by clicking the column header. The arrow next to the header name indicates

Field	Information
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Date/Time	The date and time the alert occurred.
Type	The type of alert: Firewall, Program, or Lock Enabled.
Protocol	The communications protocol used by the traffic that caused the alert.
Program	The name of the program attempting to send or receive data. (Applies only to Program alerts).
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm Pro blocked.
Destination IP	The address of the computer the blocked traffic was sent to.
Direction	The direction of the blocked traffic. "Incoming" means the traffic was sent to your computer. "Outgoing" means the traffic was sent from your computer.
Action Taken	How the traffic was handled by ZoneAlarm Pro.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Source DNS	The domain name of the computer that sent the traffic that caused the alert.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.

Adding the source of the alert to the Trusted Zone

If you determine that you received a firewall alert because ZoneAlarm Pro blocked traffic from a computer that you want to share resources with, you can add that computer to the Trusted Zone directly from the alerts list. Follow these steps:

4. Right-click the source IP address you want to add.

5. Choose **Add to Zone** and Trusted from the shortcut menu.

Submitting the alert to Zone Labs AlertAdvisor

To have Zone Labs AlertAdvisor analyze an alert for you, follow these steps:

1. Right click anywhere in the alert record you want to submit.
2. Choose **More Info** from the shortcut menu.

3 – *Entry Detail* box

The Entry Detail box displays details of the alert currently selected in the alerts list. Entry detail fields are the same as those in the alerts list, but displayed in an easily readable format.

4 – *Add to Zone/More Info*

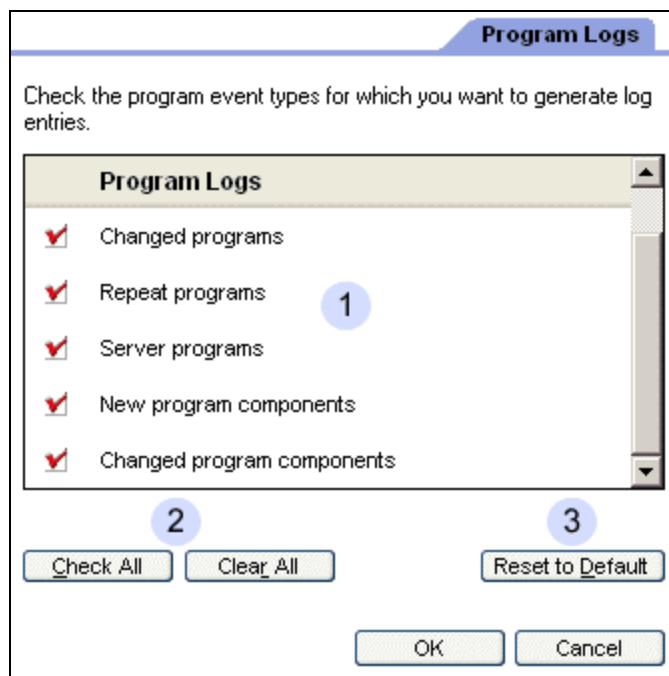
Click **Add to Zone** to add the Source IP of the selected alert to either the Blocked Zone or the Trusted Zone.

Click **More Info** to have Zone Labs' Alert Advisor analyze the selected alert, and provide advice on any action you may need to take.

5 – *Clear List*

Click **Clear List** to clear all entries from the Log Viewer. You can still view all of these entries in the ZoneAlarm Pro log.

Program Logs tab



Use the Program Logs tab to choose which types of Program alerts to record in the ZoneAlarm Pro log.

Note By default, ZoneAlarm Pro logs all program alerts. Alerts that are not recorded in the log cannot be reviewed later.

1 – Program Logs list

Select the types of Program alerts you want recorded in the ZoneAlarm Pro log. Deselect the types of Program alerts you do not want recorded in the log.

2 – Check all/clear all

Click **Check All** to have ZoneAlarm Pro display all types of Program alerts

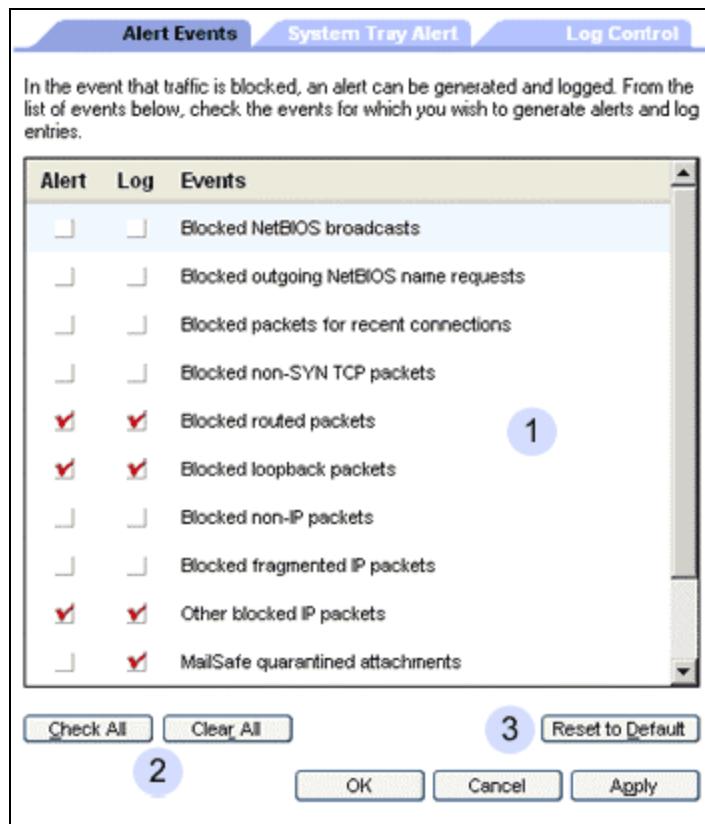
Click **Clear All** to have ZoneAlarm Pro hide all types of Program alerts

3 – Reset to default

Click **Check All** to have ZoneAlarm Pro display all types of Program alerts

Click **Clear All** to have ZoneAlarm Pro hide all types of Program alerts

Alert Events tab



Use the Alert Events tab to control in detail the display and logging of Firewall alerts, MailSafe alerts, Internet Lock alerts, and Blocked Program alerts. To open this tab, click the **Advanced** button in the Main tab of the Alerts & Logs panel.

The relationship between Main tab settings and Alert Events tab settings

The Alert Events Shown control, in the Main tab of Alerts & Logs, lets you control the display of Firewall Alerts and other alerts by rating. The **High** setting displays all alerts types, while the **Medium** setting displays only alerts probably caused by hacker activity. This control does not affect logging.

The Alert Events tab gives you more detailed control of alert display, as well as logging. You can specify which types of Firewall alerts to display and log by type of traffic blocked.

Tip New Program alerts, and the other program alerts that require a "yes" or "no" response from you, are always displayed. You can control the logging of these alerts by using the Program Logs tab.

1 – Firewall events list

For each type of event in the list:

- Select the **Alerts** box to have ZoneAlarm Pro display an alert box when that type of event occurs.
- Select the **Log** box to have ZoneAlarm Pro record the event in the log.

2 – **Check All/Clear All**

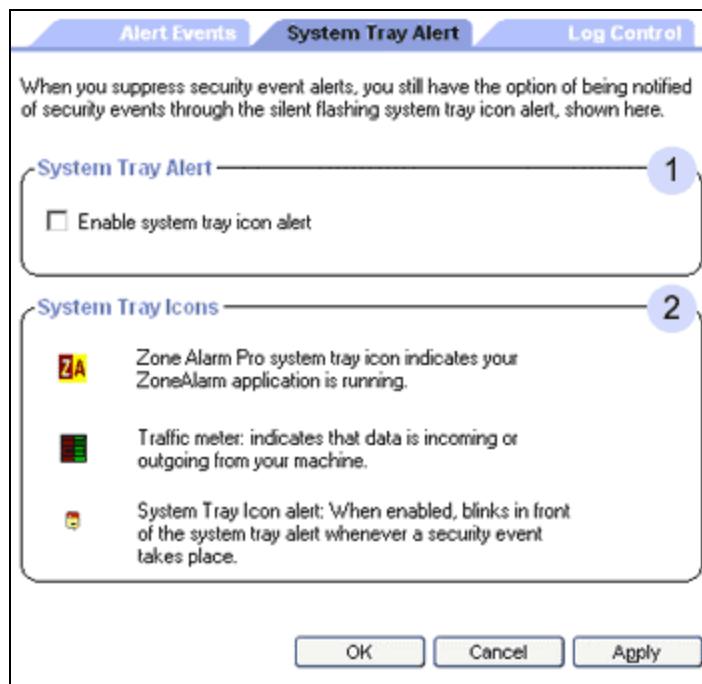
Click **Check All** to log and display alerts for all of the event types listed.

Click **Clear All** to suppress logging and alert display for all of the event types listed.

3 – **Reset to Defaults**

Click **Reset to Default** to restore settings in the Alert Events tab to their Zone Labs defaults.

System Tray Alert tab



Use the System Tray Alert tab to enable or disable the display of an alert icon in the system tray (in the lower right corner of your Windows desktop).

1 – **System Tray Alert**

When you choose to hide some or all informational alerts, ZoneAlarm Pro can still keep you aware of those alerts by showing a small alert icon in the system tray.

To have ZoneAlarm Pro display the system tray icon alert, select the check box labeled **Enable system tray icon alert**.

2 – System Tray Icons

The icons displayed in the system tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks.

To open the ZoneAlarm Pro control center, double-click any of the system tray icons.

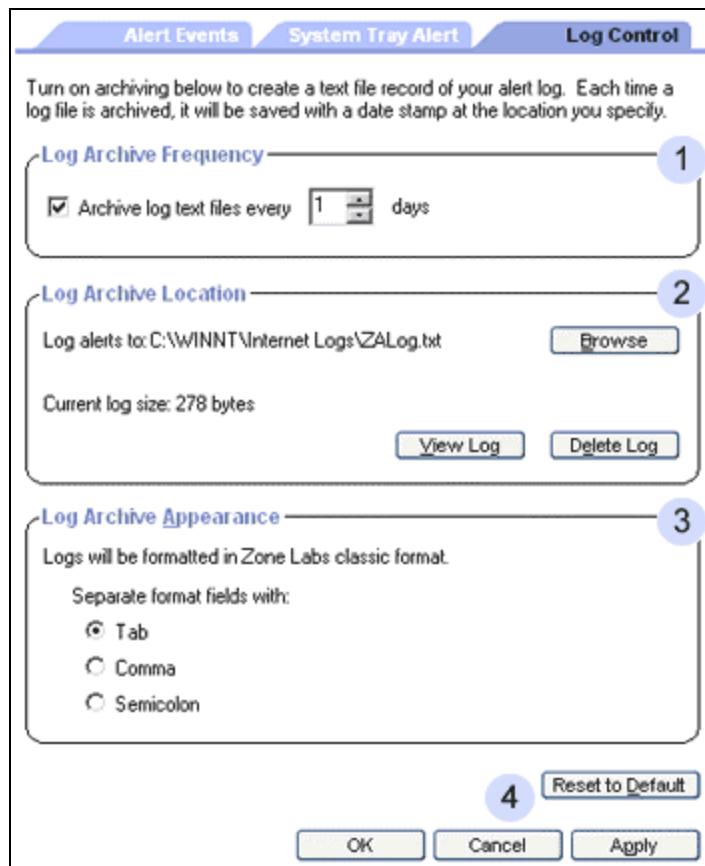
Icon	Meaning
 ZoneAlarm Pro is installed and running.	
 Your computer is sending (red band) or receiving (green band) network traffic. This indicator does not imply that you have a security problem, or that the network traffic is dangerous.	
 ZoneAlarm Pro has blocked a communication, but your settings prevent a full-sized alert from being shown.	

System Tray Menu

The system tray shortcut menu, shown below, gives you quick access to the Internet Lock and other functions. To open the menu, right-click the system tray icon.

For more information about the **Engage Internet Lock** and **Stop all Internet activity functions**, see *Using the Internet Lock and Stop button*, page 54.

Log Control tab



Use the Log Control tab to determine when, where and how ZoneAlarm Pro will save and archive log files. To access this tab, click the **Advanced** button in the Main tab of Alerts & Logs.

1 – Log Archive Frequency

To turn log archiving on and to determine how often logs will be archived, follow these steps:

1. To turn log archiving on, select the **Archive...** check box.
2. Use the spin box to select the log archive frequency.

To turn archiving off, clear the check box.

2 – Log Archive Location

ZoneAlarm Pro logs events to a text file, named ZAlog.txt.

At regular intervals, the contents of ZAlog.txt are archived to a date-stamped file, for example, ZAlog2002.02.04.txt (for February 4, 2002). This prevents ZAlog.txt from becoming unmanageably large.

The ZAlog.txt file and all archived log files are stored in the same directory. The default locations are C:\Windows\Internet Logs (for Windows 95, Windows98, Windows ME, and Windows XP); and C:\Winnt\Internet Logs (for Windows NT, Windows 2000).

Use the **Browse** button to designate the location for the current log and archived log files. You can also change the name of the log file.

Use the **View Log** button to open the current log file.

Use the **Delete Log** button to delete the current log file. This will not delete the archived log files.

Tip To view **archived** log files, use Windows Explorer to browse to the directory your logs are stored in.

3 – Log Archive Appearance

Use these controls to determine the field separator for your log files.

Select **Tab** to separate fields with a tab character.

Select **Comma** to separate log fields with a comma.

Select **Semicolon** to separate log fields with a semicolon.

4- Buttons

Click **Reset to Default** to return log control settings to Zone Labs defaults.

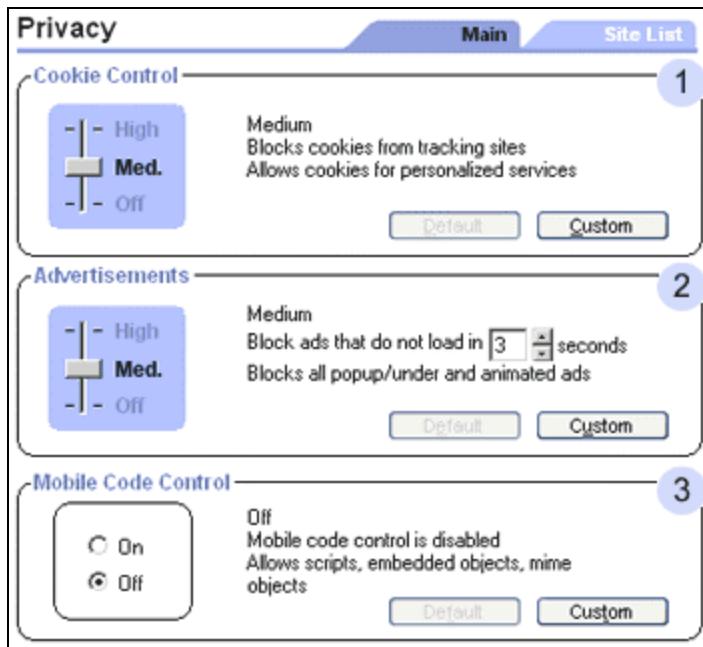
Click **Cancel** to close the dialog box without saving any changes you have made.

Click **Apply** to save your changes but leave the dialog box open.

Click **OK** to save your changes and close the dialog box.

Privacy Panel

Main tab



Use this tab to select general settings for cookie control, ad blocking, and mobile code control.

Note If you did not enable privacy during setup, the sliders on this panel will be set to **Off** rather than to their default settings. To enable privacy protection for your browser, raise the Cookie Control and/or Ad Blocking sliders to the level of protection you desire. To enable privacy protection for other programs, use the Programs tab.

1 – Cookie Control

Use the slider to select a global setting for cookie control.

ZoneAlarm Pro provides two preconfigured cookie control settings: **High** and **Medium**. The default **Medium** setting provides an optimal balance of security and convenience for most situations. Click **Custom** to open the Cookies tab, where you can customize cookie control settings.

Settings

- **High** blocks persistent cookies and third-party cookies; but allows the use of session cookies.
- **Medium** blocks third-party cookies; but allows the use of session cookies and persistent cookies.
- **Off** Allows the use of all types of cookies.

Note If you have customized your cookie control settings, the slider control is disabled. To abandon your customized settings and return to preconfigured settings, click the **Default** button.

2 – Ad Blocking

Use the slider to select a global setting for ad blocking. ZoneAlarm Pro provides two preconfigured settings: High and Medium. The default Medium setting provides an optimal balance of security and convenience for most situations.

If Medium ad blocking is selected use the spin box to set a time limit for banner and skyscraper ads to download. Click **Custom** to open the Ad blocking tab, where you can customize ad blocking settings.

Settings

- **High** blocks common types of ads (pop-up, pop-under, animated, and banner/skyscraper), whether they affect the speed at which web pages load or not.
- **Medium** blocks pop-up ads, pop-under ads and animated ads, but blocks banner and skyscraper ads only when they slow down the performance of the Web sites you visit.
- **Off** allows all advertisements.

Note If you have customized your ad blocking settings, the slider control is disabled. To abandon your customized settings and return to preconfigured settings, click the **Default** button.

3 – Mobile Code control

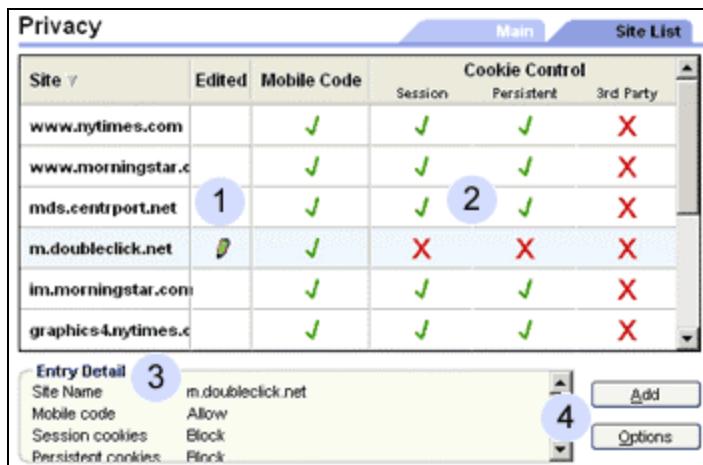
Use the radio buttons to turn mobile code on or off. Click **Custom** to open the Mobile Code tab, where you can customize mobile code control settings.

Settings

- **On** Blocks scripts, MIME-type integrated objects, and embedded objects.
- **Off** Blocks no mobile code. This is the default setting, allowing the Web interactivity supported by active controls.

Note Blocking mobile code may disable some interactive features of Web sites you visit. To abandon customized settings and return to preconfigured settings, click the **Default** button.

Site List tab



Use the Site List tab of the Privacy panel to customize cookie control and mobile code control settings for specific Web sites.

The list displays sites you have visited in your current ZoneAlarm Pro session, and sites for which you have previously customized settings. If you do not customize settings for a site you've visited, it is dropped from the list when you shut down your computer or shut down ZoneAlarm Pro.

1 – *Site/Edited*

A pencil icon in the Edited column indicates that you have customized privacy settings for that site, and the site will remain in your list.

If there is no icon in the column, the site is one you have visited in your current session, and will disappear from the list when your session ends.

2 – *Mobile Code and Cookie Control*

The site list shows two types of Web sites:

- Sites that have delivered cookies to your computer during your current Internet session.
- Sites for which you have already edited custom cookie or mobile code settings.

By default, the list is sorted by site name. You can re-sort it by setting by clicking any of the column headers. The arrow next to the header tells you whether the sort is in ascending or descending order.

Privacy symbols

Symbol	Meaning
--------	---------

	Allow the cookie or mobile code.
	Block the cookie or mobile code without notifying you

To change a privacy setting for a site, click the symbol you want to change, then choose from the shortcut menu.

Tip The general privacy settings in the Main tab of the Privacy panel are applied to any sites you don't customize privacy settings for. You don't have to customize settings for each site to be protected.

3 – *Entry Detail*

The details box displays information about the site selected in the site list. To see details for any site in the list, click on the site name.

4 – *Add/Options*

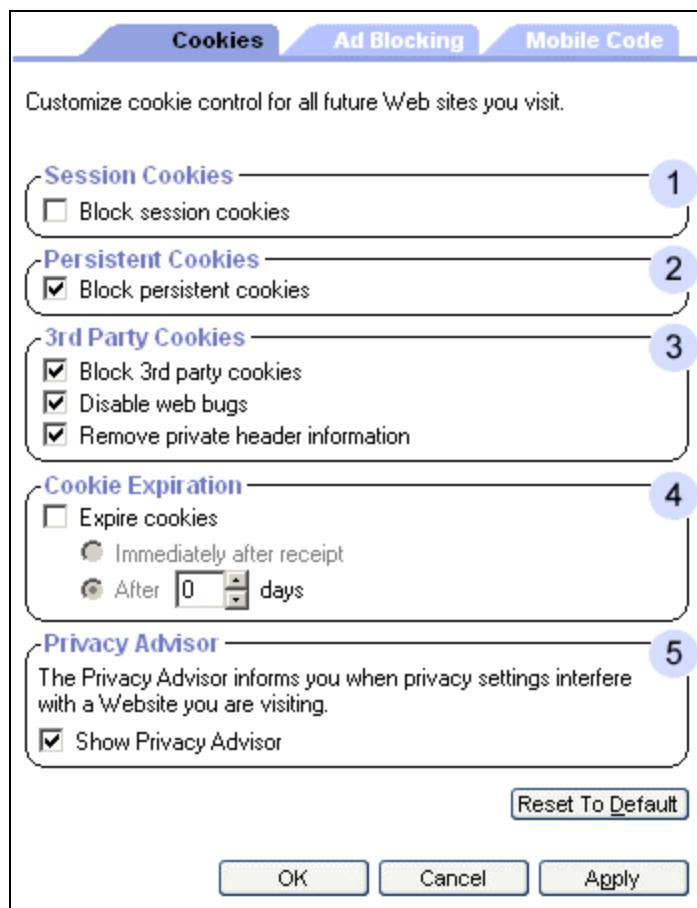
Click the **Add** button to manually add a site to the list. The Add dialog box opens.

Type the URL of the host or site in the text box provided, then click **OK**.

Setting options for a site

Click the **Options** button to open the Site Options dialog box. Use the Cookies tab, Ad blocking tab, and Mobile Code tab to customize settings for the selected site.

Cookies tab



Use this tab to customize cookie control. You can:

- Choose what types of cookies to block
- Choose the period after which persistent cookies will expire
- Enable or disable Web bugs
- Allow or block transfer of private header information

Note This tab appears in both the Site Options dialog box (for customizing a particular site) , and in the Custom Privacy Settings dialog box (for customizing defaults).

1 – Session cookies

Use this control to allow or block session cookies .

session cookie A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their short life-span.

2 – Persistent cookies

Use this control to allow or block persistent cookies.

persistent cookie A cookie put on your hard drive by a Web site you visit. These cookies can be retrieved by the web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.

3 – Third-party cookies

Use this control to allow or block third-party cookies.

third party cookie A persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other \third party.\ These cookies are commonly used to deliver information about your Internet activity to that third party.

4 – Cookie expiration

The sites that use persistent cookies may set those cookies to remain active for a few days, several months, or indefinitely. While a cookie is active, the site (or third party) that created it can use the cookie to retrieve information. After the cookie expires, it can no longer be accessed.

If you choose to allow persistent cookies, you can override their expiration dates and specify how long they will remain active before expiring.

- **Immediately after receipt** allows persistent cookies to operate during the session in which they were received only. The cookie expires as soon as you leave the site.
- **After X days** allows persistent cookies to remain active for the number of days you specify. You can choose any number from 1 to 999. The default setting is 1.

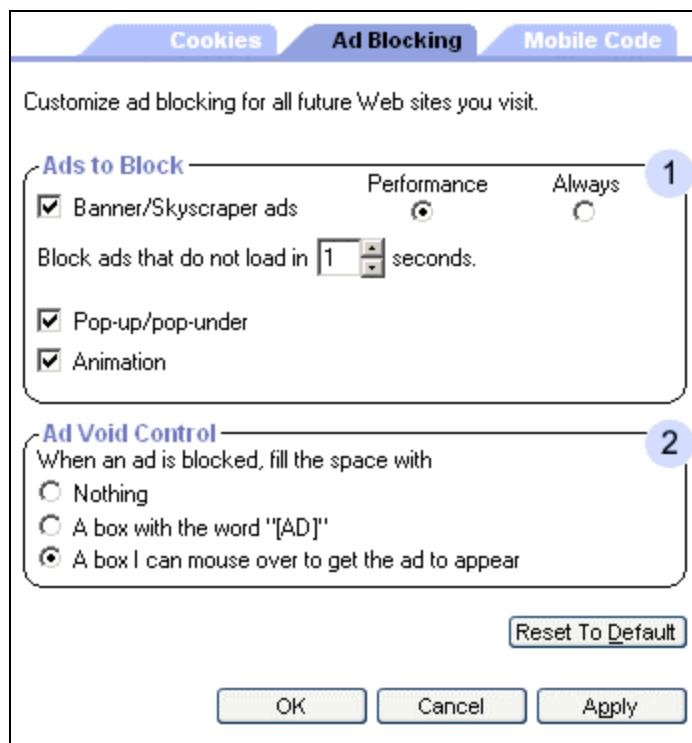
5 – Privacy Advisor Control

Use this control to enable or disable the Privacy Advisor, and to control when it will be displayed.

Select **Show Privacy Advisor** to display the advisor whenever ZoneAlarm Pro blocks cookies or mobile code.

Clear the check box to prevent the Privacy Advisor from appearing.

Ad Blocking tab



Use this tab to

- Choose what types of ads to block
- Choose what to do with the screen space in which a blocked ad was to be displayed

Note This tab appears in both the Site Options dialog box (for customizing a particular site) , and in the Custom Privacy Settings dialog box (for customizing defaults).

1 – Ads to Block

These controls let you choose which specific types of advertisements you want to block or allow.

If you choose to block banner ads and skyscraper ads:

- Choose **Always** to have those ads blocked in all cases
- Choose **Performance** to have them blocked only when the ads do not load within the amount of time specified in the counter. You can set the counter to any value from 1 to 99 seconds.

If you choose to block pop-up ads and pop-under ads, or animated ads, those advertisements are blocked in all cases, since they do not affect the speed at which Web pages load.

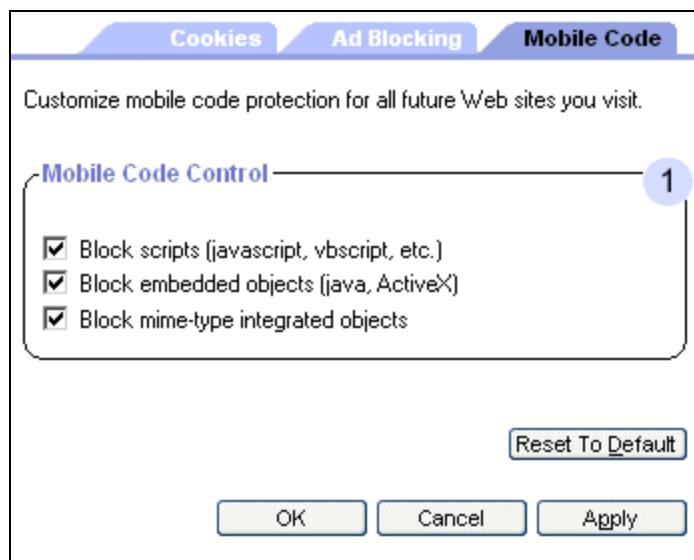
2 – Ad Void Control

When ZoneAlarm pro blocks banner, skyscraper, or animated ad, it leaves a "void" or blank on your screen where the ad was to be displayed. Ad void control lets you specify what will be displayed in that space:

- Nothing
- A box with the word [AD]
- A box you can mouse over to get the ad to appear

By default, ZoneAlarm Pro displays a box with the words "blocked ad", so that you are aware of what is happening.

Mobile Code tab



Use this tab to customize mobile code control settings by specifying which code types to allow or block:

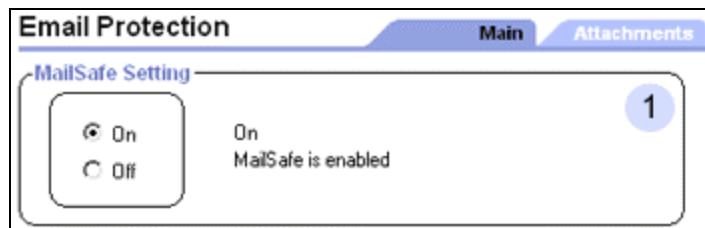
- Scripts
- MIME-type integrated objects
- Embedded objects

For definitions, see the *Glossary*.

Note This tab appears in both the Site Options dialog box (for customizing a particular site) , and in the Custom Privacy Settings dialog box (for customizing defaults).

E-mail Protection panel

Main tab

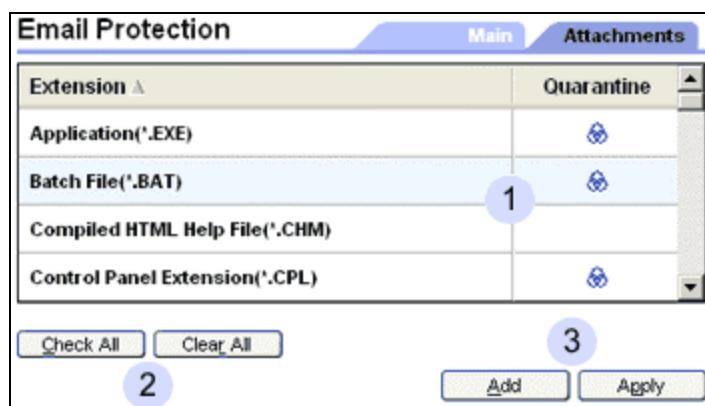


Use this tab to turn MailSafe protection on or off.

Use the radio buttons to turn MailSafe on or off.

- If **On** is selected, the attachment types configured in the Attachments panel will be quarantined.
- If **Off** is selected, no attachments will be quarantined.

Attachments tab



The Attachments tab lists the types of e-mail attachments that ZoneAlarm Pro's MailSafe feature will quarantine. Each attachment type is specified by its filename extension, for example, .EXE for applications.

Use this tab to:

- Quarantine or allow an attachment type
- Add attachment types to the list.

- Remove attachment types from the list.

Note ZoneAlarm Pro comes preconfigured with 45 attachment types that can carry worms or other harmful code. By default, ZoneAlarm Pro quarantines all of these attachment types.

1 – Extension/Quarantine

The Extension list displays the attachment types that can be quarantined.

You can sort the list by either field by clicking the column header. The arrow (↑) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

To turn the quarantine function on or off for a specific attachment type, click the Quarantine column, then choose **Quarantine** or **Allow** from the shortcut menu.

2 – Check All/ Clear All

Click **Check All** to have MailSafe quarantine all attachment types in the list.

Click **Clear All** to have MailSafe allow all attachment types in the list.

3 – Add/Apply

Click **Add** to add an attachment type to the list using the Add dialog box.

Click **Apply** to save any changes you have made in this tab.

Use the Add dialog box to add an extension to the MailSafe list. To access the Add dialog, click the **Add** button in the Attachments tab.

Type a description and filename extension (with or without the "." character), then click **OK**

6 Glossary

A

access permission

Access permission allows a program on your computer to initiate communications with another computer. This is distinct from server permission, which allows a program to "listen" for connection requests from other computers. You can give a program access permission for the Trusted Zone, the Internet Zone, or both.

Several common applications may need access permission to operate normally. For example, your browser needs access permission in order to contact your ISP's servers. Your e-mail client (for example, MS Outlook) needs access permission in order to send or receive e-mail.

The following basic options are available for each program:

Allow the program to connect to computers in the Internet Zone / Trusted Zone

Block the program from accessing computers in the Internet Zone / Trusted Zone

Ask whether the program should have access permission (show [Repeat Program alert](#))

[Back](#)

act as a server

A program acts as a server when it "listens" for connection requests from other computers. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need to act as servers to operate properly. However, some hacker programs act as servers to listen for instructions from their creators.

ZoneAlarm Pro prevents programs on your computer from acting as servers unless you grant server permission.

[Back](#)

ActiveX control

Based on Microsoft's ActiveX technology, these controls are mostly used to embed interactive elements (buttons, checkboxes, etc.) in Web pages.

Because they have full access to the Windows operating system, malicious ActiveX controls can be dangerous.

[Back](#)

ad blocking

A ZoneAlarm Pro feature that enables you to block banner, pop-up and other types of advertisements.

[Back](#)

AlertAdvisor

Zone Labs AlertAdvisor is an online utility that enables you to instantly analyze the possible causes of an alert, and helps you decide whether to respond **Yes** or **No** to a Program alert. To use AlertAdvisor, click the **More Info** button in an alert pop-up. ZoneAlarm Pro sends information about your alert to AlertAdvisor. AlertAdvisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

[Back](#)

animated ad

An advertisement that incorporates moving images.

[Back](#)

B

banner ad

An ad that appears in a horizontal banner across a Web page.

[Back](#)

Blocked Zone

The Blocked Zone contains computers you want no contact with. ZoneAlarm Pro prevents any communication between your computer and the machines in this Zone.

[Back](#)

C

component

A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

[Back](#)

cookie

A small data file used by a Web site to customize content, remember you from one visit to the next, and/or track your Internet activity. While there are many benign uses of cookies, some cookies can be used to divulge information about you without your consent.

[Back](#)

cookie control

A ZoneAlarm Pro feature that enables you to block the use of all cookies, or specific types of cookies, thus protecting you from "data leaks" stemming from cookie use.

[Back](#)

D

DHCP (Dynamic Host Configuration Protocol)

A protocol used to support dynamic IP addressing. Rather than giving you a static IP address, your ISP may assign a different IP address to you each time you log on. This allows the provider to serve a large number of customers with a relatively small number of IP addresses.

[Back](#)

DHCP (Dynamic Host Configuration Protocol) broadcast/multicast

A type of message used by a client computer on a network that uses dynamic IP addressing. When the computer comes online, if it needs an IP address, it issues a broadcast message to any DHCP servers that are on the network. When a DHCP server receives the broadcast, it assigns an IP address to the computer.

[Back](#)

dial-up connection

Connection to the Internet using a modem and an analog telephone line. The modem connects to the Internet by dialing a telephone number at the Internet Service Provider's site. This is in distinction to other connection methods, such as Digital Subscriber Lines, that do not use analog modems and do not dial telephone numbers.

[Back](#)**DLL (Dynamic Link Library)**

A library of functions that can be accessed dynamically (that is, as needed) by a Windows application.

[Back](#)**DNS (Domain Name System)**

A data query service generally used on the Internet for translating host names or domain names (like www.yoursite.com) into Internet addresses (like 123.456.789.0).

[Back](#)**E****embedded object**

An object such as a sound file or image file that is embedded in a Web page.

[Back](#)**F**

(no entries)

G**gateway**

In networking, a combination of hardware and software that links two different types of networks. For example, if you are on a home or business Local Area Network (LAN), a gateway enables the computers on your network to communicate with the Internet.

[Back](#)

gateway enforcement

A setting in the Advanced dialog of the Firewall panel. It enables a compatible gateway device to make sure that ZoneAlarm Pro is installed on all machines accessing the Internet through it.

[Back](#)

H

high-rated alert

An alert that is likely to have been caused by hacker activity. High-rated Firewall alerts display a red band at the top of the alert pop-up. In the Log Viewer, you can see if an alert was high-rated by looking in the Rating column.

[Back](#)

HTTP referrer header field

An optional field in the message that opens a Web page, containing information about the "referring document." Properly used, this field helps webmasters administer their sites. Improperly used, it can divulge your IP address, your workstation name, login name, or even (in a poorly-implemented e-commerce site) your credit card number. By selecting Remove Private Header information in the Cookies tab, you prevent this header field from transferring any information about you.

[Back](#)

I

ICMP (Internet Control Messaging Protocol)

An extension of the Internet Protocol that supports error control and informational messages. The "ping" message is a common ICMP message used to test an Internet connection.

[Back](#)

ICS (Internet Connection Sharing)

ICS is a service provided by the Windows operating system that enables networked computers to share a single connection to the Internet.

[Back](#)

Internet Zone

The Internet Zone contains all the computers in the world—except those you

have added to the Trusted Zone or Blocked Zone.

ZoneAlarm Pro applies the strictest security to the Internet Zone, keeping you safe from hackers. Meanwhile, the medium security settings of the Trusted Zone enable you to communicate easily with the computers or networks you know and trust—for example, your home network PCs, or your business network.

[Back](#)

IP address

The number that identifies your computer on the Internet, as a telephone number identifies your phone on a telephone network. It is a numeric address, usually displayed as four numbers between 0 and 255, separated by periods. For example, 172.16.100.100 could be an IP address.

Your IP address may always be the same. However, your Internet Service Provider (ISPs) may use Dynamic Host Configuration Protocol (DHCP) to assign your computer a different IP address each time you connect to the Internet.

[Back](#)

ISP (Internet Service Provider)

A company that provides access to the Internet. ISP's provide many kinds of Internet connections to consumers and business, including dial-up (connection over a regular telephone line with a modem), high-speed Digital Subscriber Lines (DSL), and cable modem.

[Back](#)

J

(no entries)

K

(no entries)

L

(no entries)

M

mail server

The remote computer from which the e-mail program on your computer retrieves e-mail messages sent to you.

[Back](#)

MD5 signature

A digital "fingerprint" used to verify the integrity of a file. If a file has been changed in any way (for example, if a program has been compromised by a hacker), its MD5 signature will change as well.

[Back](#)

medium-rated alert

An alert that was probably caused by harmless network activity, rather than by a hacker attack.

[Back](#)

MIME-type integrated object

An object such as an image, sound file, or video file that is integrated into an e-mail message. MIME stands for Multipurpose Internet Mail Extensions..

[Back](#)

mobile code

Executable content that can be embedded in Web pages or HTML e-mail. Mobile code helps make Web sites interactive, but malicious mobile code can be used to modify or steal data, and for other malevolent purposes.

[Back](#)

mobile code control

A ZoneAlarm Pro feature that enables you to block active controls and scripts on the Web sites you visit. While mobile code is common on the Internet and has many benign uses, hackers can sometimes use it for malevolent purposes.

[Back](#)

More Info button

A button that appears in ZoneAlarm Pro alerts. By clicking it, you submit

information about the alert to Zone Labs' Alert Advisor, which then displays a Web page with an analysis of the alert.

[Back](#)

N

NetBIOS (Network Basic Input/Output System)

A program that allows applications on different computers to communicate within a local network. By default, ZoneAlarm Pro allows NetBIOS traffic in the Trusted Zone, but blocks it in the Internet Zone. This enables file sharing on local networks, while protecting you from NetBIOS vulnerabilities on the Internet.

[Back](#)

O

(no entries)

P

packet

A single unit of network traffic. On "packet-switched" networks like the Internet, outgoing messages are divided into small units, sent and routed to their destinations, then reassembled on the other end. Each packet includes the IP address of the sender, and the destination IP address and port number.

[Back](#)

pass-lock

When the Internet Lock is engaged, programs given pass-lock permission can continue accessing the Internet. Access permission and server permission for all other programs are revoked until the lock is opened.

[Back](#)

persistent cookie

A cookie put on your hard drive by a Web site you visit. These cookies can be retrieved by the web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.

[Back](#)

ping

A type of ICMP message (formally "ICMP echo") used to determine whether a specific computer is connected to the Internet. A small utility program sends a simple "echo request" message to the destination IP address, and then waits for a response. If a computer at that address receives the message, it sends an "echo" back. Some Internet providers regularly "ping" their customers to see if they are still connected.

[Back](#)**pop-under ad**

An ad that appears in a new browser window that opens under the window you're looking at, so you don't see the ad until you close the original browser window.

[Back](#)**pop-up ad**

An ad that appears in a new browser window that 'pops up' in front of the window you're looking at.

[Back](#)**port**

A channel in or out of your computer. Some ports are associated with standard network protocols; for example, HTTP (Hypertext Transfer Protocol) is traditionally addressed to port 80. Port numbers range from 1 to 65535.

[Back](#)**port scan**

A technique hackers use to find unprotected computers on the Internet. Using automated tools, the hacker systematically scans the ports on all the computers in a range of IP addresses, looking for unprotected or "open" ports. Once an open port is located, the hacker can use it as an access point to break in to the unprotected computer.

[Back](#)**Privacy Advisor**

A small display that shows you when ZoneAlarm Pro blocks cookies or mobile code, and enables you to un-block those elements for a particular page.

[Back](#)

product update service

A Zone Labs subscription service that provides free updates to ZoneAlarm Pro. When you purchase ZoneAlarm Pro, you automatically receive a year's subscription to product update service.

[Back](#)

program authentication

When a program on your computer asks for Internet access, ZoneAlarm Pro examines its recorded MD5 checksum to verify that it has not been tampered with since its last request. You can set ZoneAlarm Pro to authenticate only the program itself, or the program and the shared components (such as DLLs) it uses.

[Back](#)

programs list

The list of programs to which you can assign Internet access and server permissions. The list is shown in the Programs tab of the Program Control panel. You can add programs to the list, or remove programs from it.

[Back](#)

protected system files

Windows system components that are guarded by Windows File Protection. Built in to Windows 2000 and later, file protection keeps other programs from replacing system files with anything but Microsoft-certified updates.

[Back](#)

protocol

A standardized format for sending and receiving data. Different protocols serve different purposes; for example SMTP (Simple Mail Transfer Protocol) is used for sending e-mail messages; while FTP (File Transfer Protocol) is used to send large files of different types. Each protocol is associated with a specific port, for example, FTP messages are addressed to port 21.

[Back](#)

Q

Quarantine

ZoneAlarm Pro's MailSafe quarantines incoming e-mail attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining

prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other malware that hackers distribute as e-mail attachments.

[Back](#)

R

(no entries)

S

script

A series of commands that execute automatically, without the user intervening. These usually take the form of banners, menus that change when you move your mouse over them, and popup ads.

[Back](#)

server permission

Server permission allows a program on your computer to "listen" for connection requests from other computers, in effect giving those computers the power to initiate communications with yours. This is distinct from access permission, which allows a program to initiate a communications session with another computer.

Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need server permission to operate properly. Grant server permission only to programs you're sure you trust, and that require it in order to work.

If possible, avoid granting a program server permission for the Internet Zone. If you need to accept incoming connections from only a small number of machines, add those machines to the Trusted Zone, and then allow the program server permission for the Trusted Zone only.

The following basic options are available for each program

Allow the program to listen for connection requests

Block the program from listening for connection requests

Ask me whether to allow the program to listen for connection requests
(show [Server Program alert](#))

[Back](#)

session cookie

A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their short life-span.

[Back](#)

skyscraper ad

An ad that appears in a vertical column along the side of a Web page.

[Back](#)

stealth mode

When ZoneAlarm Pro puts your computer in stealth mode, any uninvited traffic receives no response—not even an acknowledgement that your computer exists. This renders your computer invisible to other computers on the Internet, until permitted program on your computer initiates contact.

[Back](#)

T**third party cookie**

A persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other 'third party.' These cookies are commonly used to deliver information about your Internet activity to that third party.

[Back](#)

Trojan horse

A malicious program that masquerades as something useful or harmless, such as a screen saver. Some Trojan horses operate by setting themselves up as servers on your computer, listening for connections from the outside. If a hacker succeeds in contacting the program, he can effectively take control of your computer. This is why it's important to only give server permission to programs you know and trust. Other Trojan horses attempt to contact a remote address automatically.

[Back](#)

TrueVector security engine

The primary component of ZoneAlarm Pro security. It is the TrueVector engine that examines Internet traffic and enforces security rules.

[Back](#)

Trusted Zone

The Trusted Zone contains computers you trust want to share resources with.

For example, if you have three home PCs that are linked together in an Ethernet network, you can put each individual computer or the entire network adapter subnet in the ZoneAlarm Pro Trusted Zone. The Trusted Zone's default medium security settings enable you to safely share files, printers, and other resources over the home network. Hackers are confined to the Internet Zone, where high security settings keep you safe.

[Back](#)

U

(no entries)

V

Virtual Private Network (VPN)

A network that is constructed by using public wires to connect nodes. When using VPN over the Internet, encryption and other security mechanisms are used to ensure that only authorized users can access the network and the data.

[Back](#)

W

web bug

An image file, often 1x1 pixel, designed to monitor visits to the page (or HTML e-mail) containing it. Web bugs are used to find out what advertisements and Web pages you have viewed.

[Back](#)

XYZ

(no entries)

